User Guide

ion4xi_WP

HFCL

Table of Contents

List of Figures

List of Tables

1 Introduction

ion4xi_WP is a cloud managed 2x2:2 MU-MIMO Wi-Fi 6 certified Access Point with a sleek and aesthetic design that raises the bar for wireless performance and efficiency. Designed especially for the Hospitality industry, the Wall Plate Access Point ensures high speeds, great network coverage & ultra-secure connectivity. ion4xi_WP is ideal for most demanding use cases and high performance-intensive applications like high-definition videos & high bandwidth requirements thereby ensuring enhanced guest experience.

1.1 Product Specifications

Parameter	ion4xi_WP
Peak Throughput	Up to 1.78 Gbps
Wi-Fi Standard Support	802.11 a/b/g/n/ac/ac Wave 2/ax
Ethernet support/ Ports/Interface	• 1 X 10/100/1000/2500 BASE-T Ethernet (WAN & PoE-In) • 4 X 10/100/1000 BASE-T Ethernet (LAN) • DC input jack (optional) • Reset and WPS buttons
MU-MIMO	2x2:2
Mesh Support	Self-creating, Self-healing EasyMesh
Maximum number of SSID (per radio)	16
Maximum User Support	256
Power Supply	IEEE 802.3af PoE or +12V DC Power Adaptor (optional)
Power Consumption (Max)	15 W (approx.)
Max Transmit Power	2.4 GHz- up to 20 dBm & 5 GHz- up to 23 dBm (will depend on country specific guidelines)
Antenna Type	Integrated antennas
Antenna Gain	4 dBi for both 2.4 GHz and 5 GHz
Management	Standalone (via GUI) or through on-premises based solution or cloud-based
Enclosure Dimensions	163 x 150 x 38 mm (6.4 x 5.9 x 1.49 inch)
Weight	0.59 kg
Operating Temperature	0°C to 40°C
Certifications	FCC Class B, CE, Passpoint 3.0, EasyMesh, WPA3, RoHS 3.0

Table 1: Product Specifications

1.2 Federal Communication Commission Certified

The APs are tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If these equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

1.2.1 FCC Caution

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could avoid the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

1.2.2 FCC Radiation Exposure Statement

- This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.
- These devices complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
  - These devices may not cause harmful interference.
  - These devices must accept any interference received, including interference that may cause undesired operation.

1.3 Make in India

These devices complies with **Make in India** standards.

1.4 Safety

Observe the following safety precautions and avoid damage to the access point:

- Do not power the device during installation
- Keep away from high voltage cables
- Keep away from high temperature
- Disconnect the device from power source before cleaning
- Do not use damp cloth for wiping
- Do not power off the unit in the middle of an upgrade process
- Do not open the enclosure
- Fasten the device tightly

2 ion4xi_WP (Dual Band 2x2:2 Indoor Wall Plate Access Point)

2.1.1 Front View

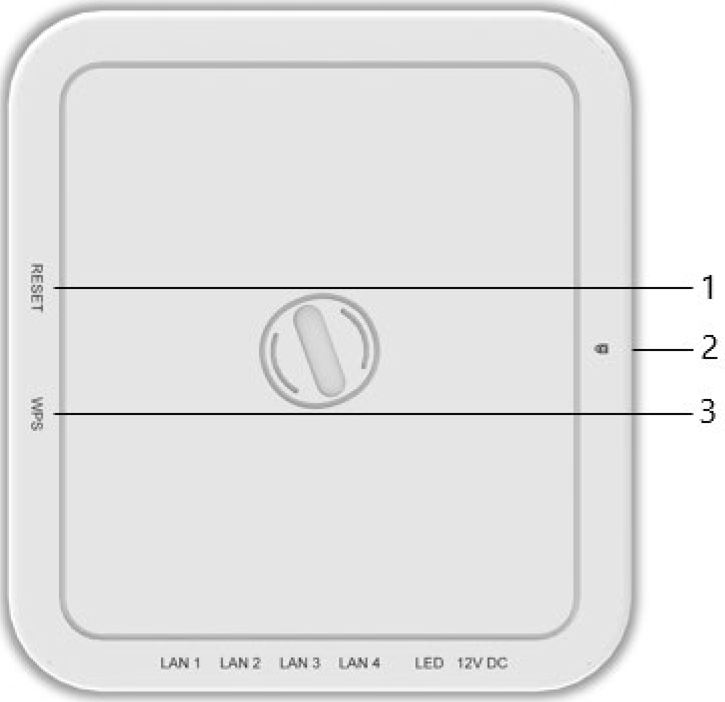


Figure 1: ion4xi_WP Front View

Call Out	Name	Description
1.	Reset button	To reset the device
2.	Kensington Lock	Provides extra physical security in device
3.	WPS button	Wi-Fi Protected Setup sync button

Table 2: ion4xi_WP Front View Description

2.1.2 Connector View

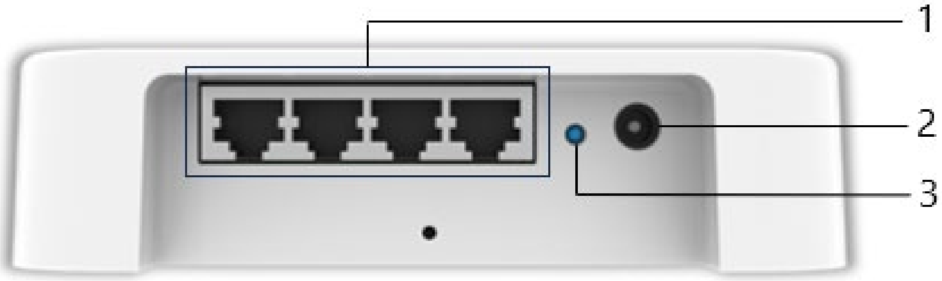


Figure 2: ion4xi_WP Connector View

Call Out	Name	Description
1.	4 LAN Ports	4 x 1 Gigabit Ethernet LAN ports
2.	DC Jack	Power up using 12V adaptor
3.	Status and Power LED	**Status LED Blue (Constant)** - Solid/constant blue color notifies the user that the device is powered ON and no data is being transmitted.

		Status LED Blue (Slow blinking) - Slow blinking blue color notifies the user that the device is powered ON and data is being transmitted on either one or both radios
		Status LED Blue (Fast blinking) - Fast blinking blue color notifies the user that the device is rebooting

Table 3: ion4xi_WP Connector View Description

2.1.3 Back View

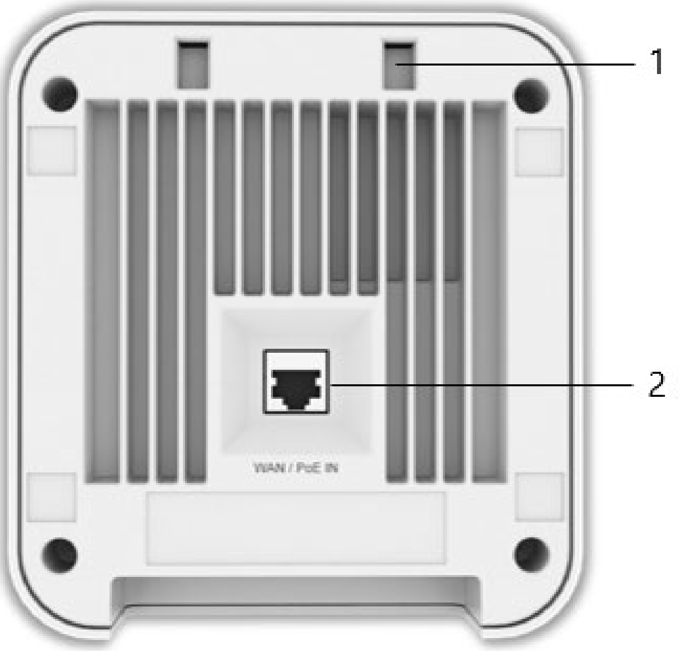


Figure 3: ion4xi_WP Back View

Call Out	Name	Description
1.	Mounting Slots	Helps in device mounting
2.	WAN + PoE Port	Power up the device by PoE adaptor and a WAN port

Table 4: ion4xi_WP Back View Description

3 Initial Setup

3.1 System Requirements

Before installing the access point, make sure that your system includes the following:

- 10/100/1000 Mbps local area network device such as a hub or switch
- The Category 5 UTP straight-through Ethernet cable with RJ-45 connector
- We can power up the device through PoE adaptor which should be 803at/af compliant
- 100–240 V, 50–60 Hz AC power source
- A web browser to configure the devices
- At least 802.11b/g-compliant devices

3.2 Packaging Content

The box contains the following items:

- ion4xi_WP Access Point
- Mounting Accessories

3.3 Connect to the Indoor Access Point

Follow the steps mentioned below and connect to the indoor AP through GUI:

1. Power up the device using PoE adaptor or DC adaptor.
2. Configure a computer with a 1-domain static IP address e.g. 192.168.1.10 and a subnet mask of 255.255.255.0.
3. For help configuring a static IP address on your computer, check the instructions or online help that came with that computer.
4. Connect the Ethernet cable to the computer.
5. Connect the other end of the Ethernet cable to the PoE adaptor (Data/In port). Use the unused port (P+D/Out) of PoE adaptor and connect it to the WAN/PoE IN port of the device.

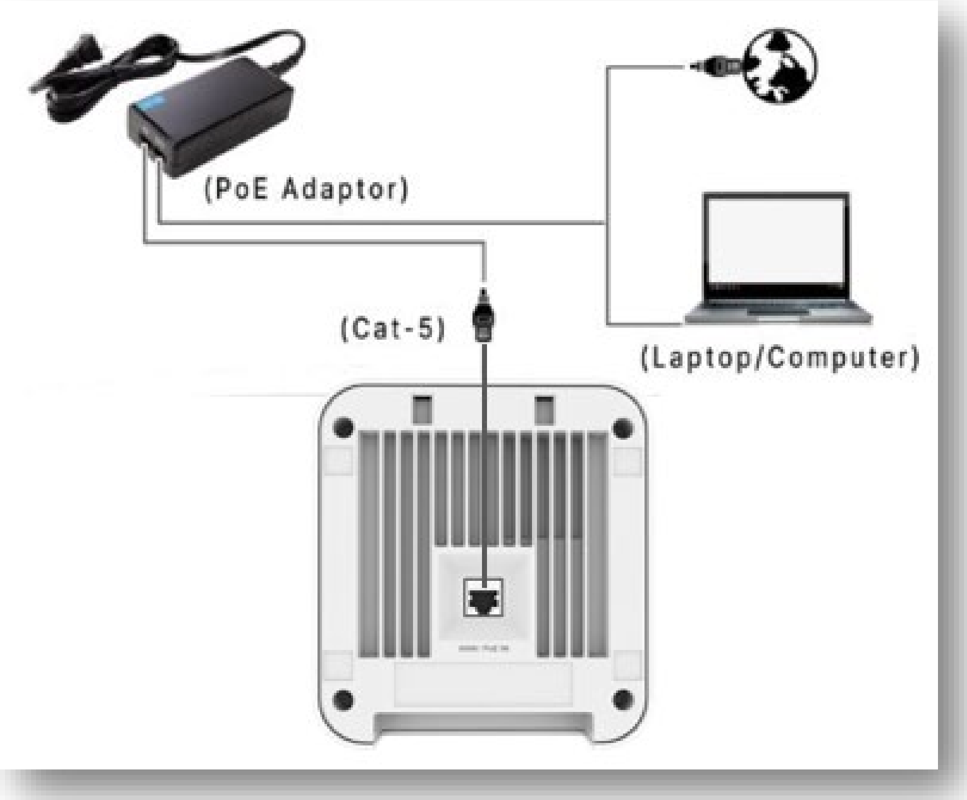


Figure 4: Connect to the Indoor Access Point

The device will be powered On.

6. Open a web browser and enter the “AP static IP address” (192.168.1.1) in the address bar.

A login screen will appear. Refer Connect to Thick Access Point and Login for more information.

4 Installation Setup

ion4xi_WP can be mounted onto the wall. Perform the steps discussed below for the appropriate installation of **ion4xi_WP**:

1. The Access Point comes with a pre-attached wall mounting bracket.

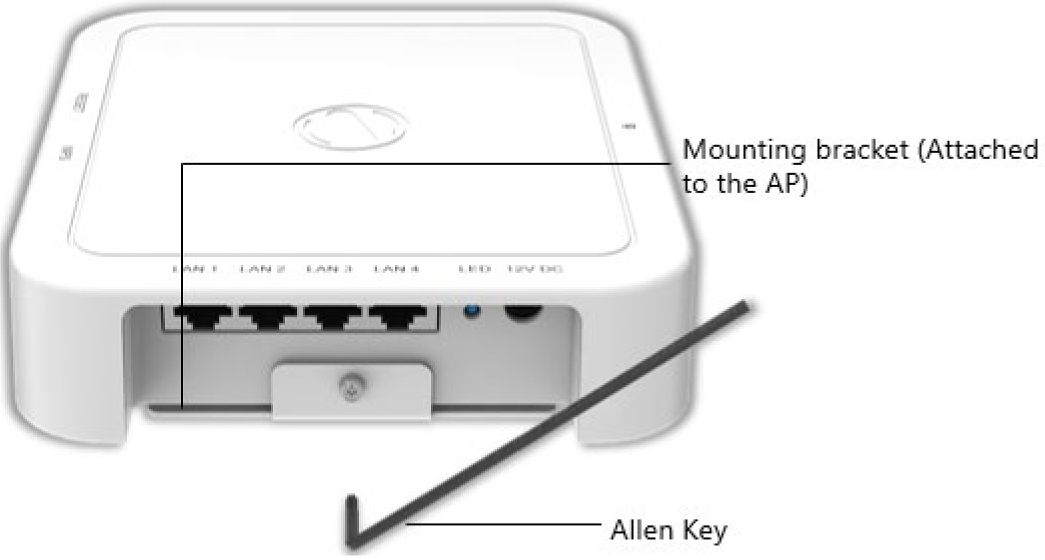


Figure 5: Attaching parts for wall mounting of ion4xi_WP

2. Use Allen Key to unscrew the wall mounting bracket from the Access Point.

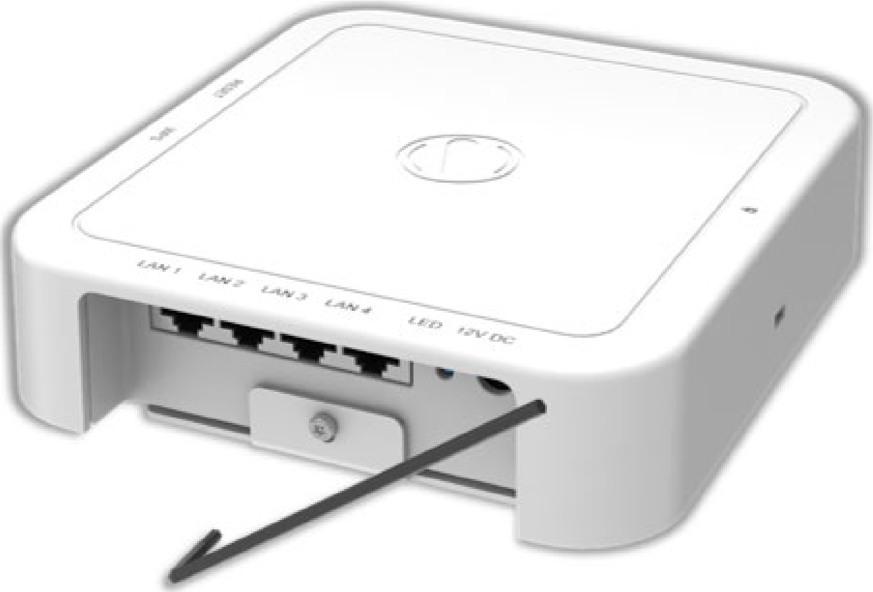


Figure 6: Unscrewing the Mounting Bracket of ion4xi_WP

An electrical wall box should be pre-installed with an Ethernet cable running from the box to a Switch with PoE.

3. There are several mounting holes on the bracket that may be used with various wall boxes. Attach the bracket on the wall using the wall mount screws

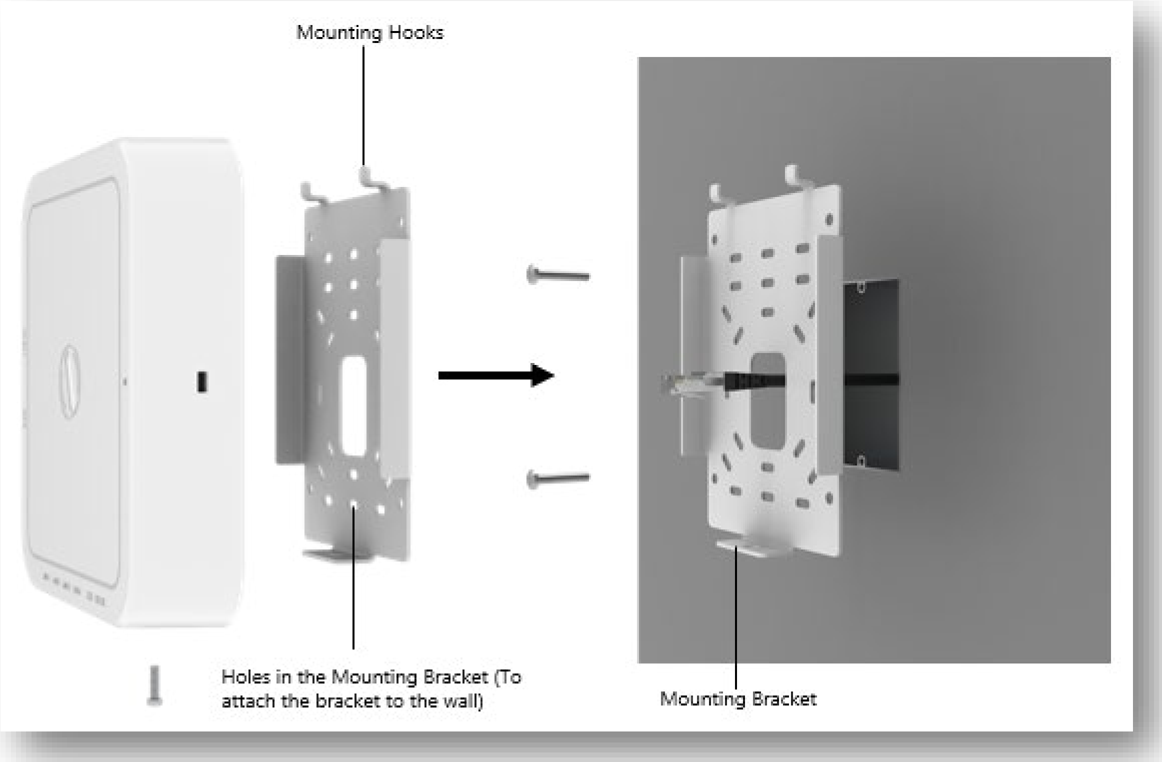

Mounting Hooks
Holes in the Mounting Bracket (To attach the bracket to the wall)
Mounting Bracket

Figure 7: Attaching bracket on to the wall

Note: Make sure that the mounting bracket is tightly installed before mounting the Access Point on the wall.

4. Pass the Ethernet cable through the bracket and connect it to the PoE port on the Access Point.

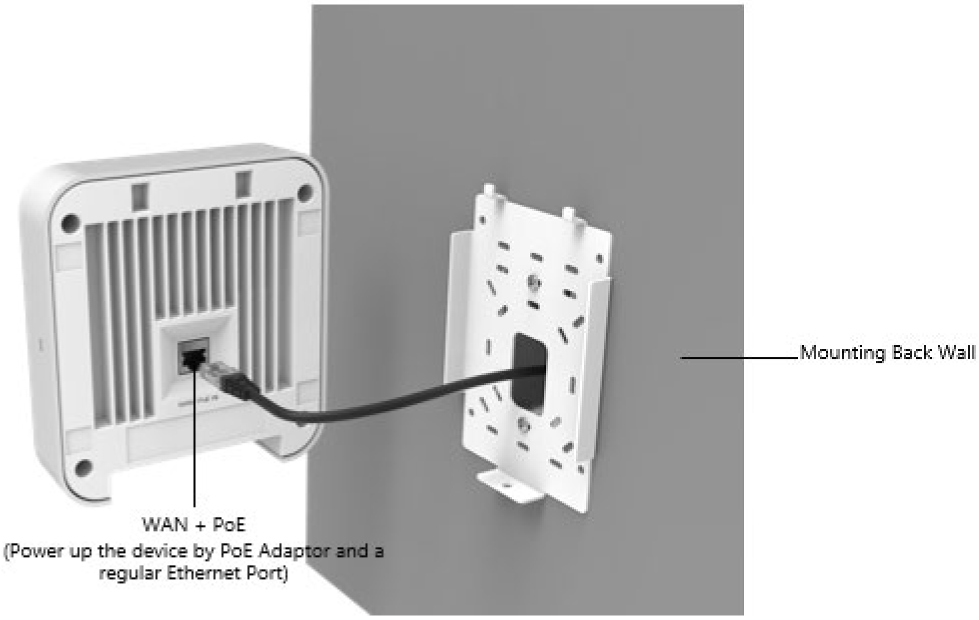

Mounting Back Wall
WAN + PoE
(Power up the device by PoE Adaptor and a regular Ethernet Port)

Figure 8: Alignment of mounting bracket with indoor AP

5 Connect to Thick Access Point and Log In

The user can connect to the access point's web management interface to view or change its LAN and wireless access settings.

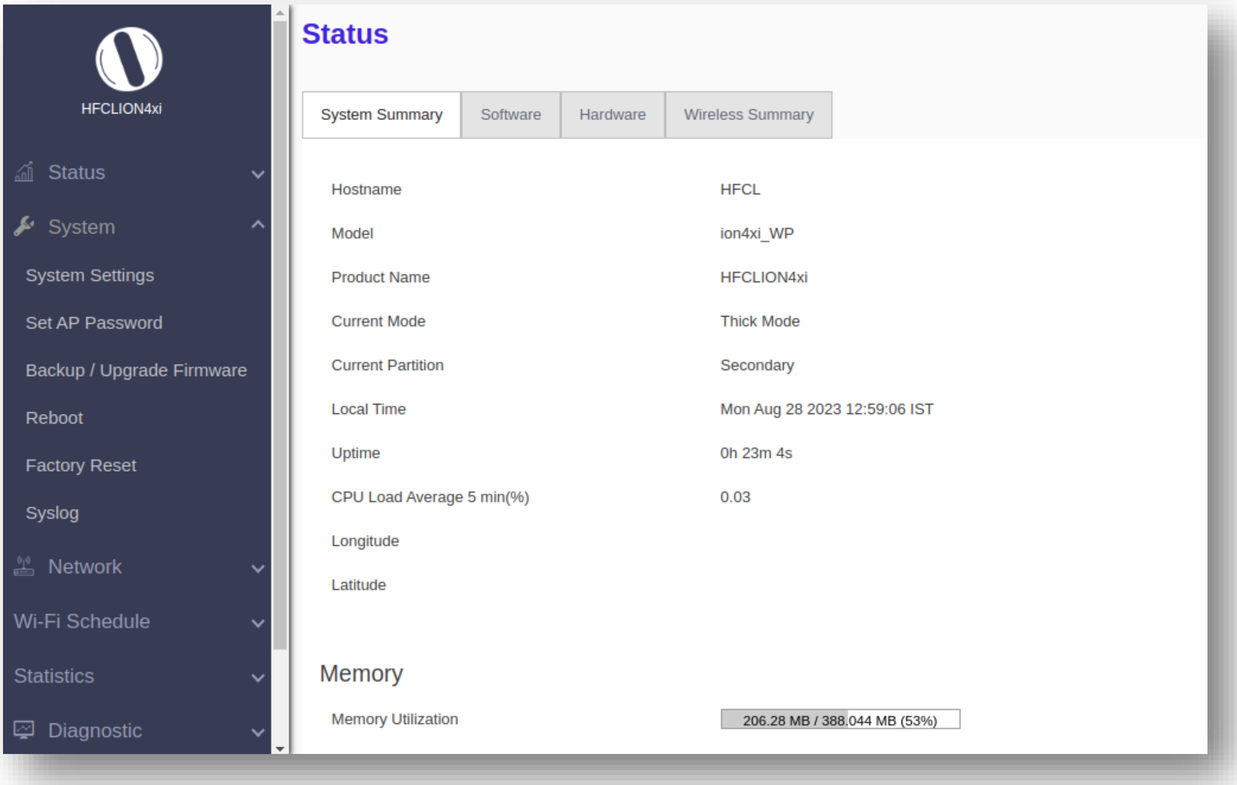
5.1 Login through GUI

This is the first screen of AP GUI. It provides access to the users with valid login credentials only. The login credentials will determine the access rights of the user.

5.2 Dashboard

On the successful device set up and login the user can view the **Dashboard** with the following options in the left pane

- Status
- System
- Network
- Wi-Fi Schedule
- Statistics
- Diagnostic
- Switch AP Mode
- Logout



Status

Hostname	HFCL
Model	ion4xi_WP
Product Name	HFCLION4xi
Current Mode	Thick Mode
Current Partition	Secondary
Local Time	Mon Aug 28 2023 12:59:06 IST
Uptime	0h 23m 4s
CPU Load Average 5 min(%)	0.03
Longitude	
Latitude	

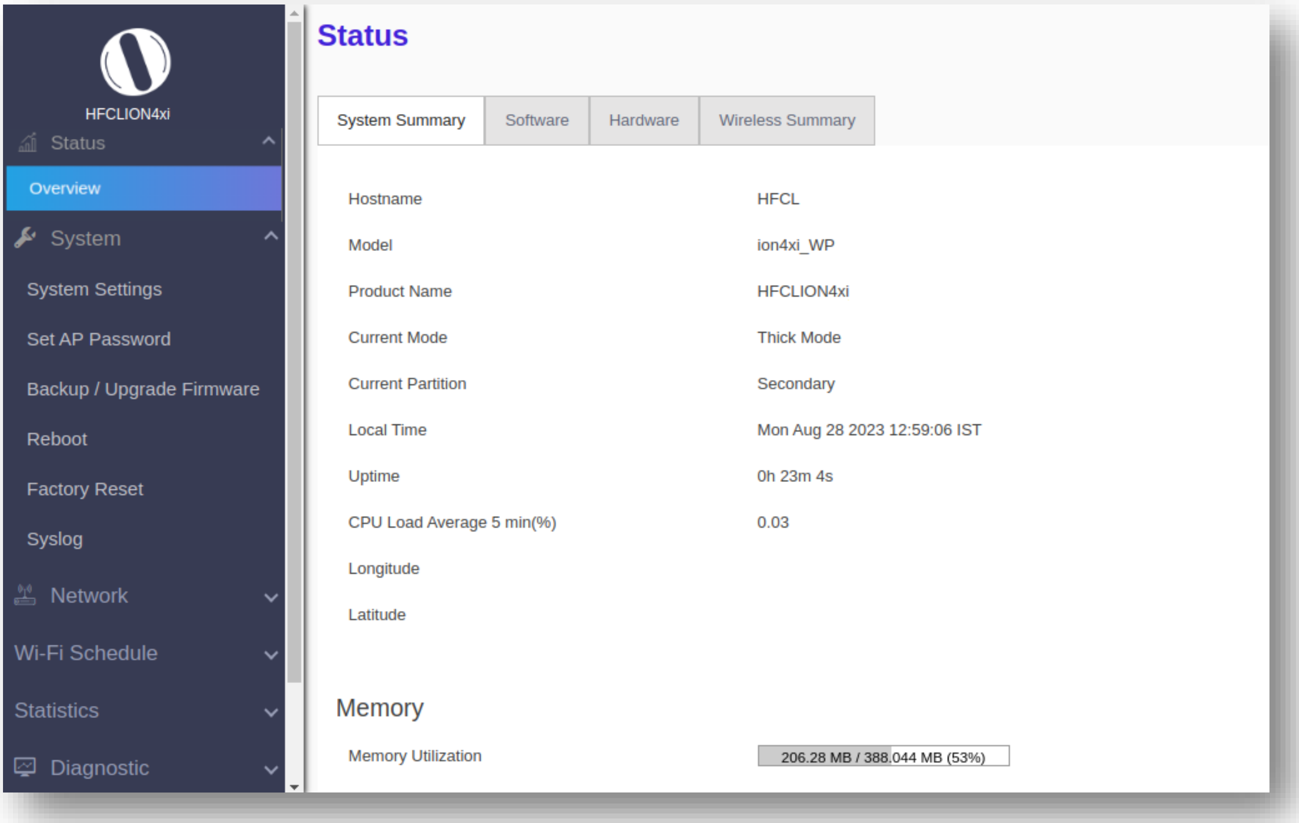
Memory

Memory Utilization	206.28 MB / 388.044 MB (53%)

Figure 9: Device Dashboard

5.3 Status

The **Status** page provides a summary of the system, software, hardware, and wireless configurations under **Overview**.



Hostname	HFCL
Model	ion4xi_WP
Product Name	HFCLION4xi
Current Mode	Thick Mode
Current Partition	Secondary
Local Time	Mon Aug 28 2023 12:59:06 IST
Uptime	0h 23m 4s
CPU Load Average 5 min(%)	0.03
Longitude	
Latitude	

Memory

Memory Utilization 206.28 MB / 388.044 MB (53%)

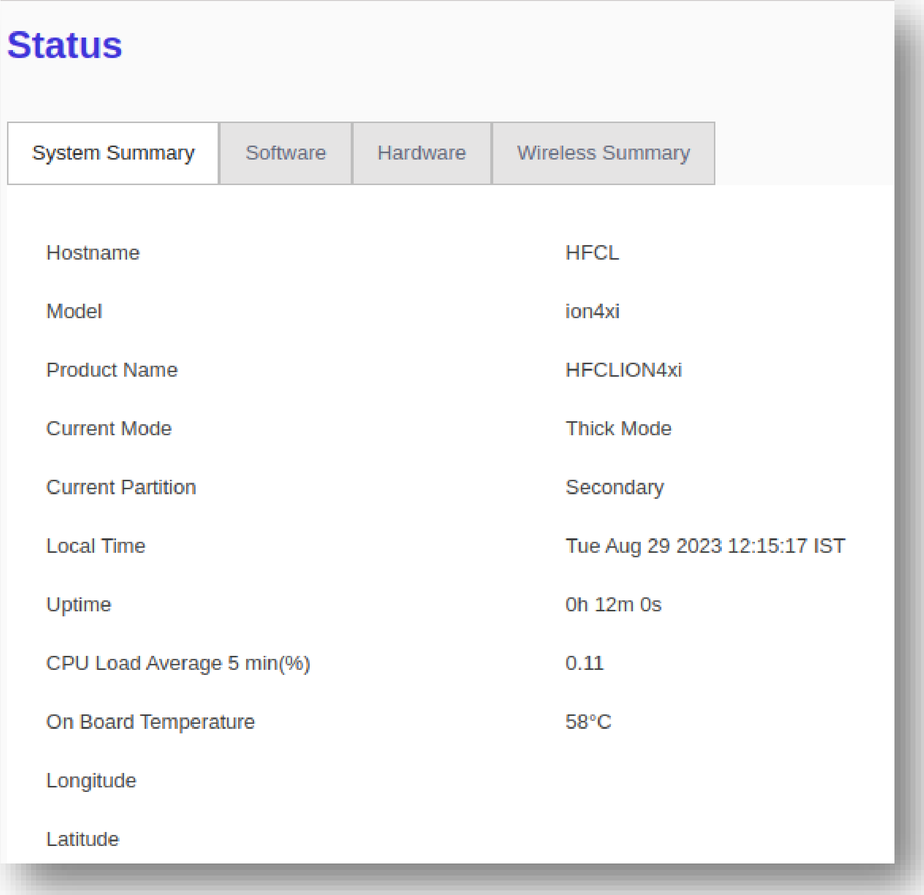
Figure 10: Status Screen

S.No.	Field	Description
1.	System Summary	Gives a brief overview of both the device and the software settings such as current mode from a bird's eye view.
2.	Software	Gives the details regarding the software.
3.	Hardware	Provides current hardware configuration details.
4.	Wireless Summary	Gives a succinct overview of the wireless specifications.

Table 5: Status Screen Description

5.3.1 System Summary

System Summary provides a detailed overview of the system specifications including **Model Number**, **Product Name**, **Uptime** along with a basic insight to the **Memory Allocation** and **Network Specifications** (IPv4 and IPv6).

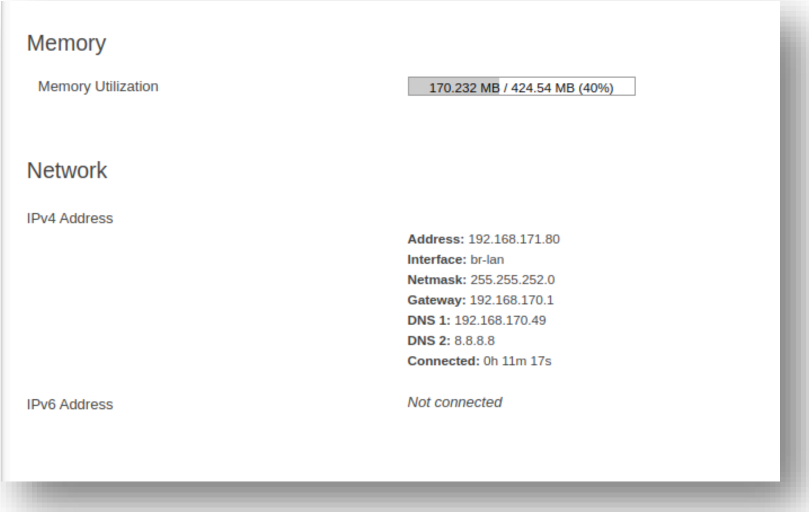


Hostname	HFCL
Model	ion4xi
Product Name	HFCLION4xi
Current Mode	Thick Mode
Current Partition	Secondary
Local Time	Tue Aug 29 2023 12:15:17 IST
Uptime	0h 12m 0s
CPU Load Average 5 min(%)	0.11
On Board Temperature	58°C
Longitude	
Latitude	

Figure 11: System Summary

S.No.	Field	Description
1.	Hostname	Current hostname of the software as configured
2.	Model	Model of the ion4xi_WP
3.	Product Name	Product name of the model
4.	Current Mode	The current mode of the software (either Thick or Thin mode)
5.	Current Partition	Primary or Secondary
6.	Local Time	Current local time as per the software.
7.	Uptime	The time duration from the last downtime period
8.	CPU Load Average 5 min (%)	The current CPU Load Average of the last 5 minutes

Table 6: System Summary Description



Memory

Memory Utilization 170.232 MB / 424.54 MB (40%)

Network

IPv4 Address

Address: 192.168.171.80
Interface: br-lan
Netmask: 255.255.252.0
Gateway: 192.168.170.1
DNS 1: 192.168.170.49
DNS 2: 8.8.8.8
Connected: 0h 11m 17s

IPv6 Address *Not connected*

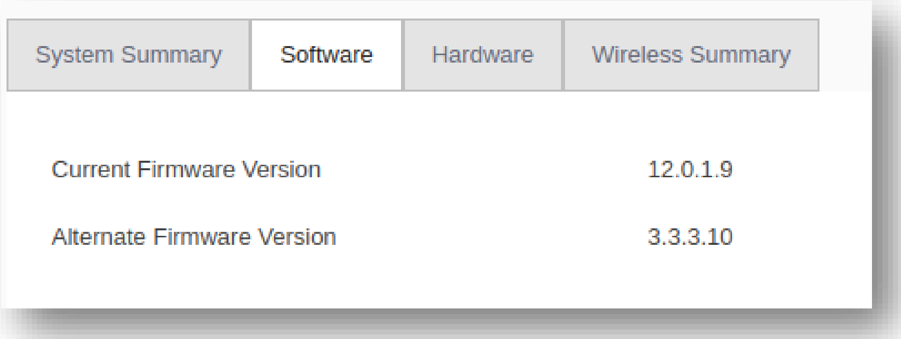
Figure 12: Memory & Network Allocations

S.No.	Field	Description
1.	Memory	Memory occupied shown in percentage.
2.	Network	Gives information on IPv4 address and IPv6 network specifications such as current interface, gateway, and IP address, etc.
3.	IPv4 Address	Displays the allocated IPv4 address
4.	IPv6 Address	Displays the allocated IPv6 address

Table 7: Memory & Network Specifications Description

5.3.2 System Software

The **Software** option provides the **Current Firmware Version** of the device and an **Alternate Firmware Version**.



Current Firmware Version 12.0.1.9

Alternate Firmware Version 3.3.3.10

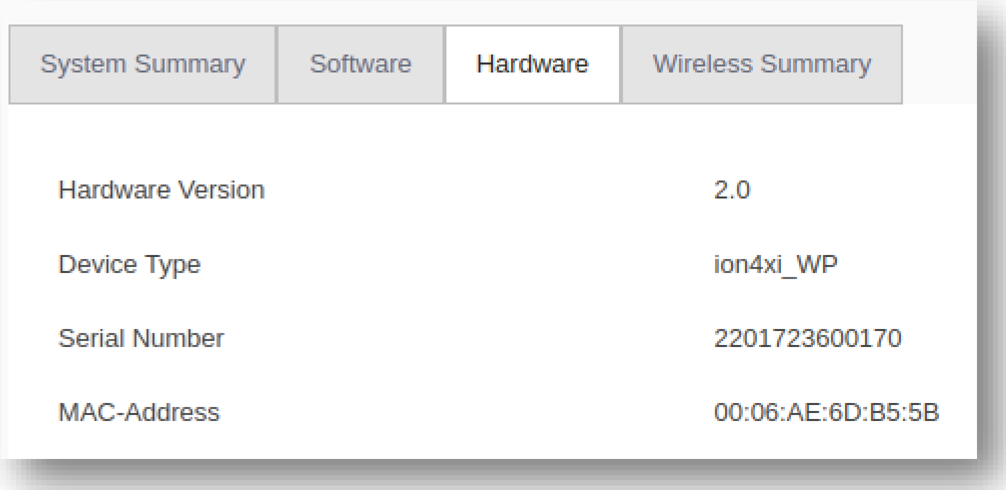
Figure 13: Software Specifications

S.No.	Field	Description
1.	Current Firmware Version	Current firmware version of the device.
2.	Alternate Firmware Version	Alternate firmware version that user can update to.

Table 8: Software Specifications Description

5.3.3 System Hardware

The **Hardware** option provides the specifications including the specific device deployed like **Hardware Version**, **Device Type**, **MAC Address** of the particular device and its **Serial Number**.



Hardware Version	2.0
Device Type	ion4xi_WP
Serial Number	2201723600170
MAC-Address	00:06:AE:6D:B5:5B

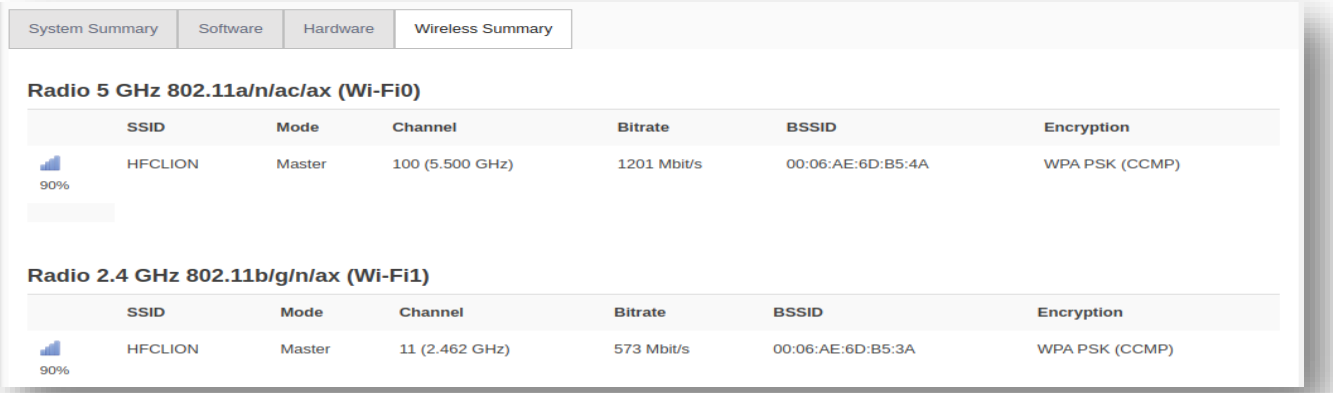
Figure 14: Hardware Specifications

S.No.	Field	Description
1.	Hardware Version	Hardware version of the device.
2.	Device Type	Family of device types that this device belongs to (different from Product Name).
3.	Serial Number	Serial number (device ID) of the device.
4.	MAC Address	MAC address of the device.

Table 9: Hardware Specifications Description

5.3.4 Wireless Summary

The **Wireless Summary** provides specification such as **SSID**, **Mode** (Master/Client), **Channel**, **BSSID**, **Bitrate** and **Encryption** enforced on the wireless frequency bands of both Radio 2.4 GHz 802.11b/g/n/ax (Wi-Fi0) and Radio 5 GHz 802.11a/n/ac/ax (Wi-Fi1) are depicted.



Radio 5 GHz 802.11a/n/ac/ax (Wi-Fi0)

	SSID	Mode	Channel	Bitrate	BSSID	Encryption
90%	HFCLION	Master	100 (5.500 GHz)	1201 Mbit/s	00:06:AE:6D:B5:4A	WPA PSK (CCMP)

Radio 2.4 GHz 802.11b/g/n/ax (Wi-Fi1)

	SSID	Mode	Channel	Bitrate	BSSID	Encryption
90%	HFCLION	Master	11 (2.462 GHz)	573 Mbit/s	00:06:AE:6D:B5:3A	WPA PSK (CCMP)

Figure 15: Wireless Summary

S.No.	Field	Description
1.	Radio 2.4 GHz (Wi-Fi0)	Depicts the current configuration of the Radio 2.4 GHz 802.11b/g/n/ax (Wi-Fi0) such as the SSIDs created of the devices, their respective modes (Client / Master) and the encryption enabled, respectively.
2.	Radio 5GHz (Wi-Fi1)	Depicts the current configuration of the Radio 5 GHz 802.11a/n/ac/ax (Wi-Fi1) such as the SSIDs created of the devices, their respective modes (Client / Master) and the encryption enabled, respectively.

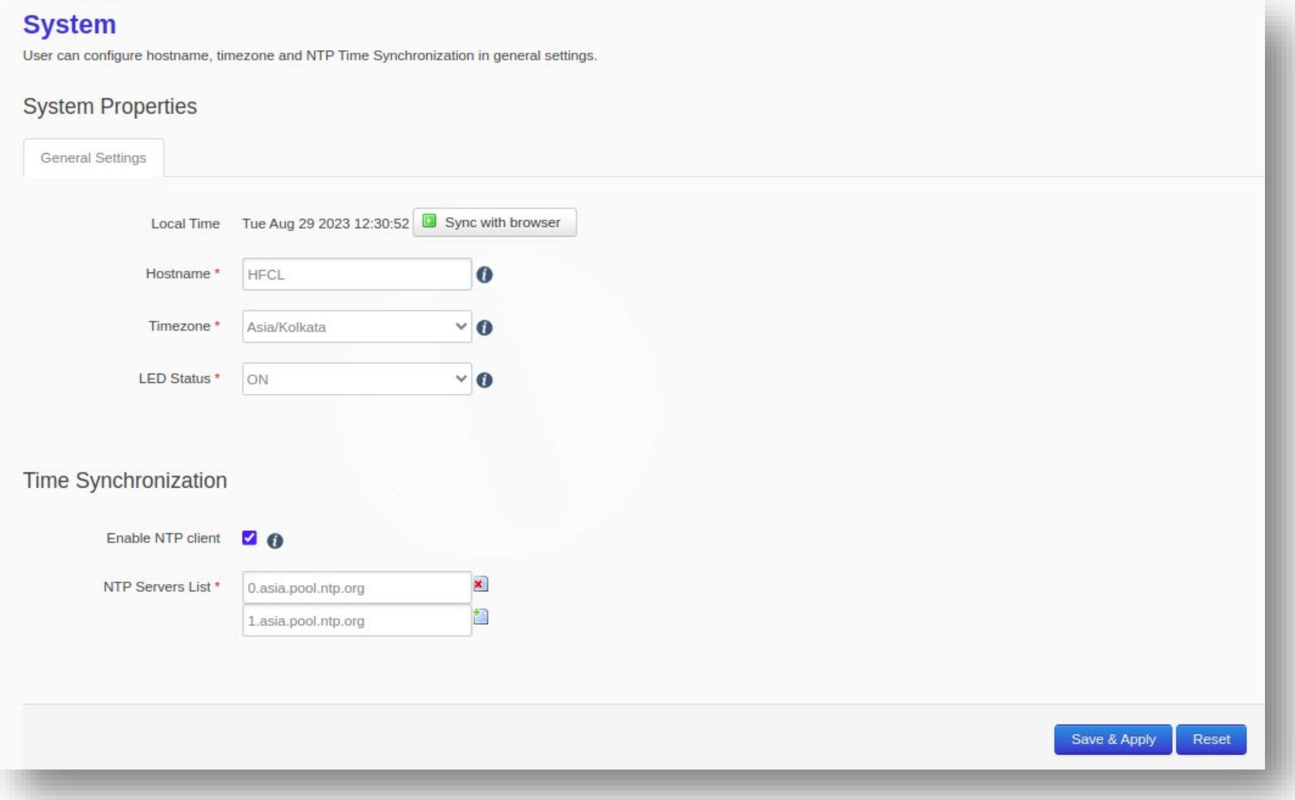
Table 10: Wireless Summary Description

5.4 System

System allows the end users to configure the system settings for the device. It has the following 6 tabs. It enables the users to configure the system settings like **Administrator Password**, **Factory Reset** and to apply updated firmware with backups.

- System Settings
- Set AP Password
- Backup/ Upgrade Firmware
- Reboot
- Factory Reset
- Syslog

5.4.1 System Settings



System

User can configure hostname, timezone and NTP Time Synchronization in general settings.

System Properties

General Settings

Local Time: Tue Aug 29 2023 12:30:52 [Sync with browser]

Hostname *: HFCL

Timezone *: Asia/Kolkata

LED Status *: ON

Time Synchronization

Enable NTP client: ☑

NTP Servers List *: 0.asia.pool.ntp.org
1.asia.pool.ntp.org

Figure 16: System Settings

Users can

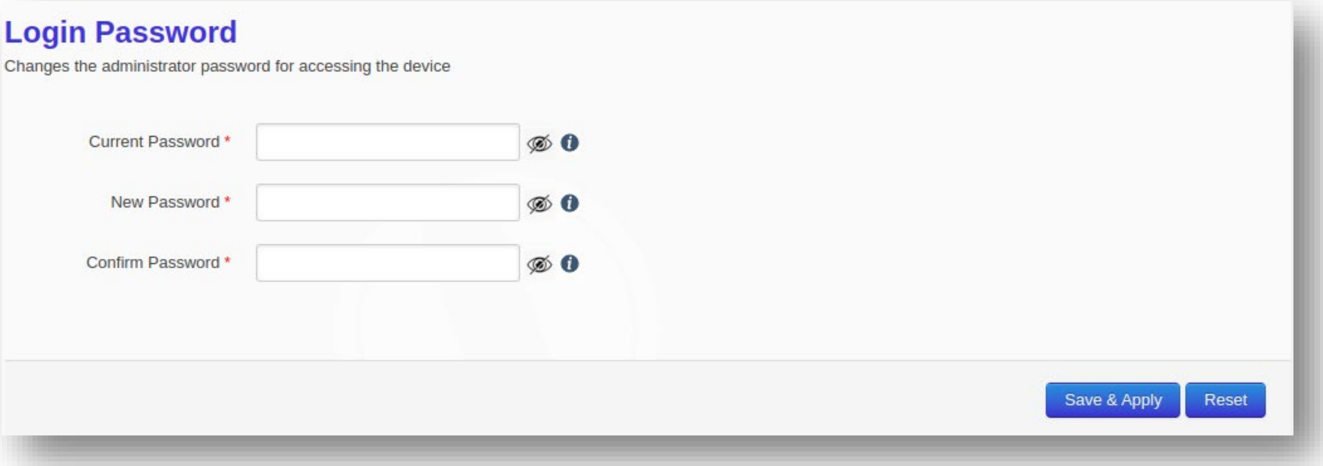
- configure the **Hostnames**
- enable syncing local time with browser and **Time zones**
- enable **NTP Client** where a maximum of 5 NTP servers can be enabled
- populate **NTP servers List** can be populated according to the user specification

S.No.	Field	Description
1.	Local Time	The current local time according to the software is displayed (which can be synchronized with the local time of the browser if required).
2.	Hostname	The host name of the software can be configured.
3.	Time zone	Time Zone of the user can be configured here.
4.	Time synchronization	Allows user to synchronize computer clock time sources in the network.
5.	Enable NTP Client	Users can opt for time synchronization using this button.
6.	NTP Servers List	If time synchronization has been enabled, then users can choose and select from the NTP Servers List as per user's requirement.
7.	Save & Apply	All changes to the configuration will be saved here and then applied.
8.	Reset	Any configuration changes made but not saved and applied will be reset.

Table 11: System Settings Description

5.4.2 Set AP Password for thick AP

The user can configure the Administrator password to access the devices.



Login Password

Changes the administrator password for accessing the device

Current Password *

New Password *

Confirm Password *

Figure 17: Set AP Password Screen

S.No.	Field	Description
1.	Set AP Password	Changes the administrator password for accessing the device.
2.	Login Password	Allows login configurations to be made and applied as per user's specifications.

3.	Current Password	Current password set to access the device.
4.	New Password	New password that the user wants to specify for the device access.
5.	Confirm Password	Password confirmation.
6.	Save & Apply	All changes to the configuration will be saved here and then applied.
7.	Reset	Any configuration changes made but not saved and applied will be reset.

Table 12: Set AP Password Description

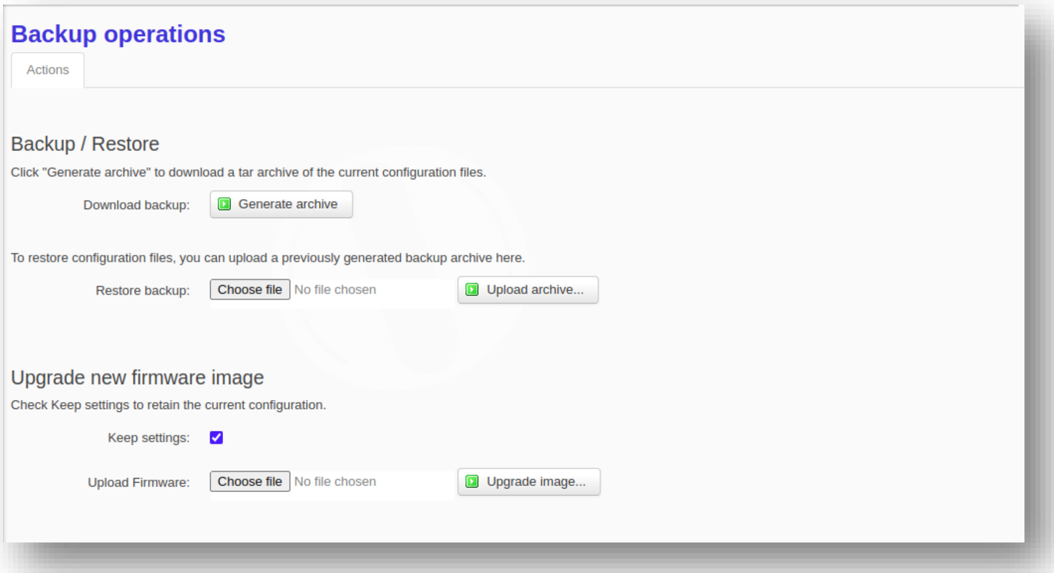
5.4.3 Backup/ Upgrade Firmware

5.4.3.1 Backup/ Restore

- Enables users to perform actions such as restoring configuration files by uploading previously generated backup archives.
- Users can also create an archive of the current configuration files which can be used to implement backups in case of failovers.

5.4.3.2 Firmware Upgrade

The firmware is stored in flash memory and can be updated with new versions to include new features or to modify the existing one. This AP has two partitions. The firmware version is always uploaded in the alternate partition to keep the current firmware image restored which is located in the current partition of access point. When we upgrade new firmware, the existing firmware will become backup firmware. If any issues are found in new firmware, the backup firmware will be booted.



Backup operations

Backup / Restore

Click "Generate archive" to download a tar archive of the current configuration files.

Download backup:

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup: No file chosen

Upgrade new firmware image

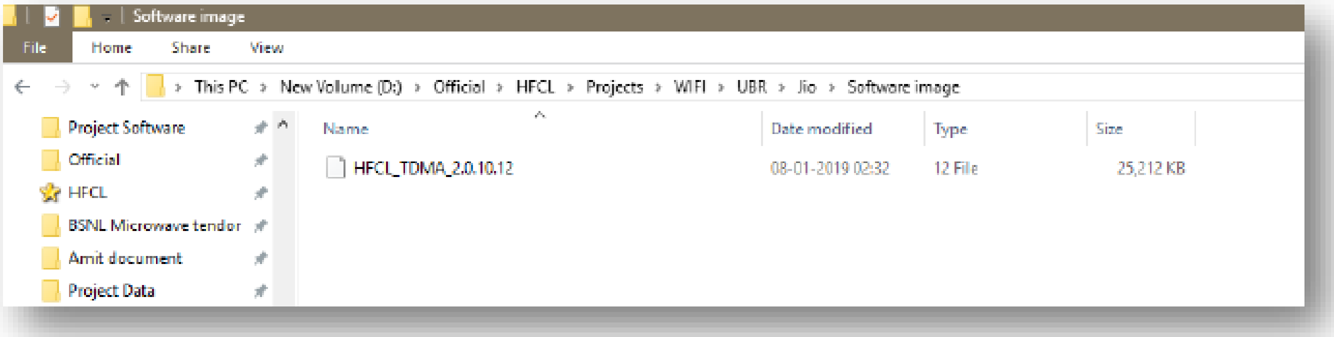
Check Keep settings to retain the current configuration.

Keep settings: ☑

Upload Firmware: No file chosen

Figure 18: Backup/Upgrade Firmware

The user can also Save the software file in the system drive. Refer the image below:



This PC > New Volume (D:) > Official > HFCL > Projects > WIFI > UBR > Jio > Software image

Name	Date modified	Type	Size
HFCL_TDMA_2.0.10.12	08-01-2019 02:32	12 File	25,212 KB

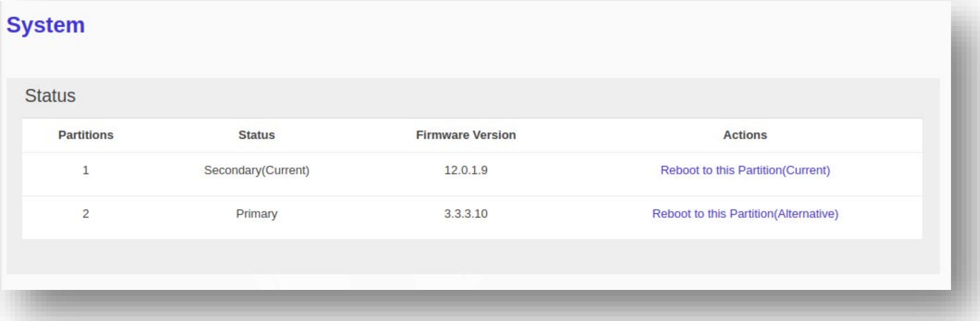
Figure 19: Upload Archive

S.No.	Field	Description
1.	Backup/Upgrade Firmware	Current firmware of the device can be upgraded and backups of the same can be created.
2.	Backup Operations	Enables users to perform backup operations.
3.	Backup/Restore	Allows user the feature of creating backups of current configuration files and restoring the same.
4.	Generate archive	Downloads a tar archive of the current configuration files if user wishes to create a backup.
5.	Restore backup-Choose File	Any previous backup can also be restored by uploading a previously generated backup archive.
6.	Upload archive	Users can upload the backup archive which needs to be restored.
7.	Upgrade new firmware image	Firmware image to be uploaded here for firmware upgrade.
8.	Keep Settings	Check this to retain the current configuration.
9.	Upload Firmware- Choose File	Upload the firmware image desired.
10.	Upgrade Image	Upgrade the current firmware image.

Table 13: Backup/Upgrade Firmware Description

5.4.4 Reboot

Reboot restarts the device with existing configuration. The user can change the firmware when the device is rebooted with different partitions. Based on the selected partition, the corresponding firmware will be loaded into the device as working firmware.


System

Status

Partitions	Status	Firmware Version	Actions
1	Secondary(Current)	12.0.1.9	Reboot to this Partition(Current)
2	Primary	3.3.3.10	Reboot to this Partition(Alternative)

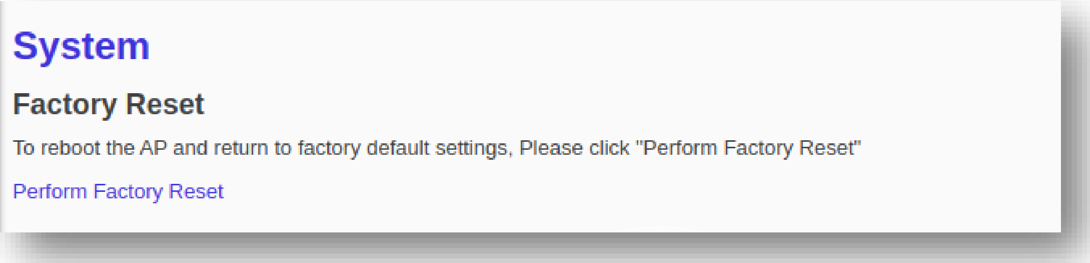
Figure 20: Reboot Screen

S.No.	Field	Description
1.	Reboot	Device can be rebooted if user desires.
2.	Partition	Displays the partition number.
3.	Status	Displays status of the device system such as Primary, Secondary.
4.	Firmware Version	Displays the current firmware version of the specific partition.
5.	Actions	Enables users to reboot to this specific partition.

Table 14: Reboot Description

5.4.5 Factory Reset

The device has factory assigned settings and configurations on deployment. The user can set the device to the same from this screen. The device will be configured back to factory settings and the existing settings and configurations will be discarded. It is recommended to take backup before setting the device to factory reset.



System

Factory Reset

To reboot the AP and return to factory default settings, Please click "Perform Factory Reset"

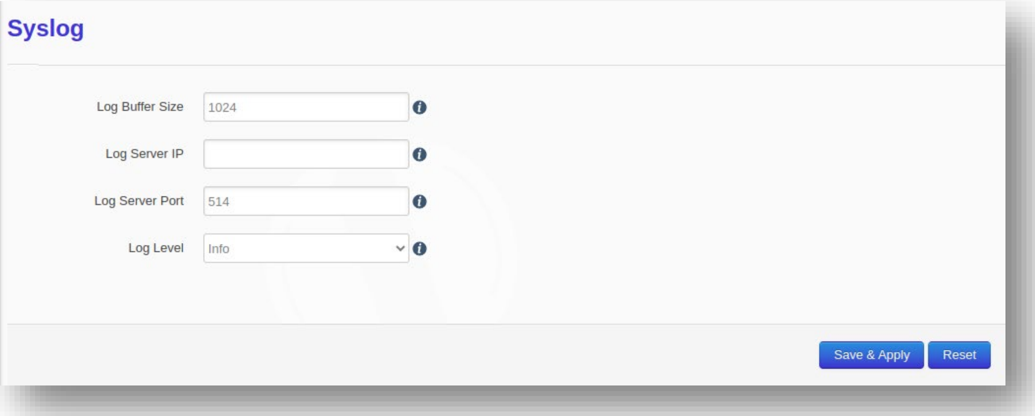
Figure 21: Factory Reset Screen

S.No.	Field	Description
1.	Factory Reset	Enables the users to make the device revert back to the factory settings (default settings).

Table 15: Factory Reset Description

5.4.6 Syslog

This page enables users to create their own syslog.



Syslog

Log Buffer Size: 1024

Log Server IP:

Log Server Port: 514

Log Level: Info

Figure 22: Syslog Screen

S.No.	Field	Description
1.	Logout	Users can log out of this application (GUI).
2.	Syslog	Provides the user with the system logs.
3.	Log Buffer Size	Create buffer size with range of 16 to 1024 kB, with a default value of 1024 kB.
4.	Log Server IP	Server IP where the syslog are to be rendered. Both IPv4 and IPv6 can be configured.
5.	Log Server Post	Users can specify the port within the range of 0 to 65353; default port as 514.
6.	Log Level	Logs all messages with a level greater than or equal to the selected one. For example, setting the priority threshold to DEBUG (lowest priority) causes all messages to be logged.

Table 16: Syslog Description

Enables users to create their own syslog according to the user specified parameters, such as

- Log Buffer Size
- Log Server IP
- Log Server Port
- Log Level
    - Critical
    - Debug
    - Info
    - Notice
    - Warning
    - Error
    - Alert
    - Emergency

S.No.	Field	Description
1.	Alert	Logs which need the users to be informed about something or alerted.
2.	Info	Logs pertaining to information.
3.	Critical	For critical logs of high priority.
4.	Debug	Logs related to debugging.
5.	Notice	Notification related logs.
6.	Warning	For logs which are warning related.
7.	Error	For error related logs.
8.	Emergency	For highest level priority concerns.

Table 17: Log Level Description

Logs all messages with a level greater than or equal to the selected one. For example, setting the priority threshold to DEBUG (lowest priority) causes all messages to be logged.

5.5 Network

The Network tab, has been further segregated into 5 divisions:

- Wireless

- Interfaces
- Easy Mesh Configuration
- DHCP Server configuration
- Static Routes

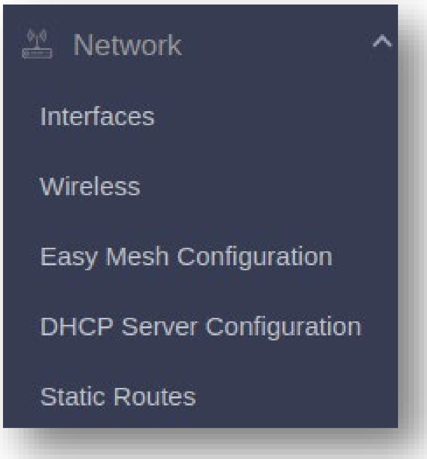
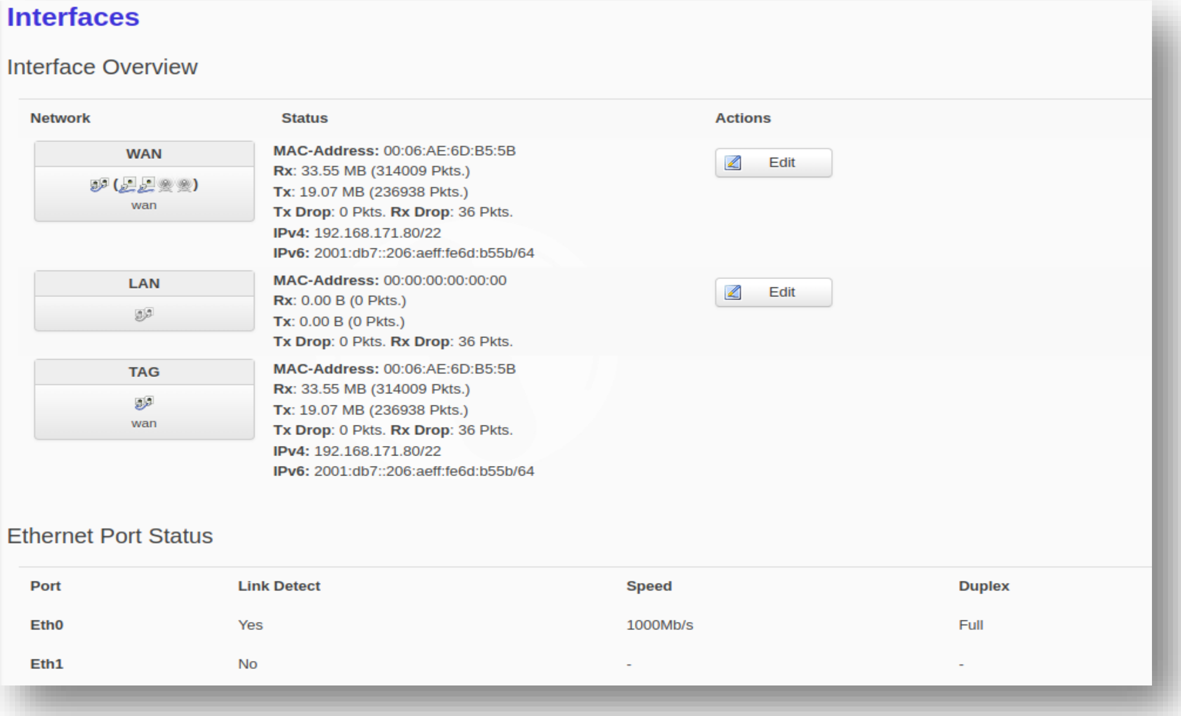


Figure 23: Network Screen

5.5.1 Interfaces

The Interface tab depicts the Interface overview and the Ethernet Port status.



Interfaces

Interface Overview

Network	Status	Actions
WAN wan	**MAC-Address:** 00:06:AE:6D:B5:5B **Rx**: 33.55 MB (314009 Pkts.) **Tx**: 19.07 MB (236938 Pkts.) **Tx Drop**: 0 Pkts. **Rx Drop**: 36 Pkts. **IPv4:** 192.168.171.80/22 **IPv6:** 2001:db7::206:aeff:fe6d:b55b/64	Edit
LAN	**MAC-Address:** 00:00:00:00:00:00 **Rx**: 0.00 B (0 Pkts.) **Tx**: 0.00 B (0 Pkts.) **Tx Drop**: 0 Pkts. **Rx Drop**: 36 Pkts.	Edit
TAG wan	**MAC-Address:** 00:06:AE:6D:B5:5B **Rx**: 33.55 MB (314009 Pkts.) **Tx**: 19.07 MB (236938 Pkts.) **Tx Drop**: 0 Pkts. **Rx Drop**: 36 Pkts. **IPv4:** 192.168.171.80/22 **IPv6:** 2001:db7::206:aeff:fe6d:b55b/64	

Ethernet Port Status

Port	Link Detect	Speed	Duplex
Eth0	Yes	1000Mb/s	Full
Eth1	No	-	-

Figure 24: Interface Screen

S.No.	Field	Description
1.	Interface Overview	Gives information of the interfaces of the device.
2.	Network	Gives the interface name.
3.	Status	Displays the interface specific information.
4.	Actions	Allows users to make configuration changes pertaining to the interface.
5.	Ethernet Port Status	Displays the current ports of the device.
6.	Port	Gives the port name.
7.	Link Detect Speed	Informs if Link Detect has been enabled or not and its respective speeds.

Table 18: Interface Description

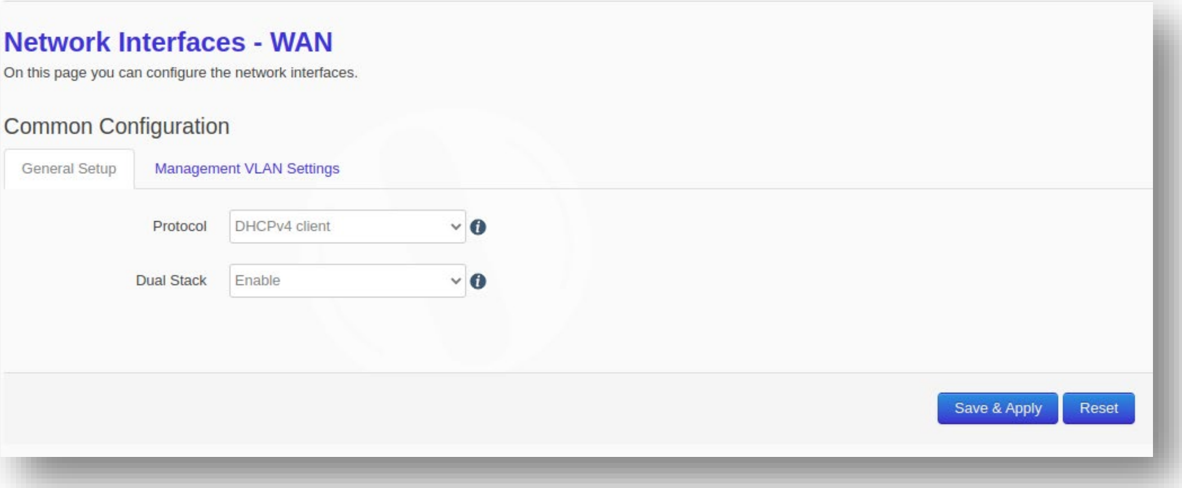
Information regarding the network connected, its status (MAC address, Transaction information and IPv4) is displayed. Users can also edit the interface and can configure the same according to their requirements.

5.5.1.1 Network Interfaces

In this Interface page of setting, user can configure the network interfaces. It has two subdivisions:

- General Setup
- Management VLAN Settings

5.5.1.1.1 Network Interface: General Setup



Network Interfaces - WAN

On this page you can configure the network interfaces.

Common Configuration

Protocol: DHCPv4 client

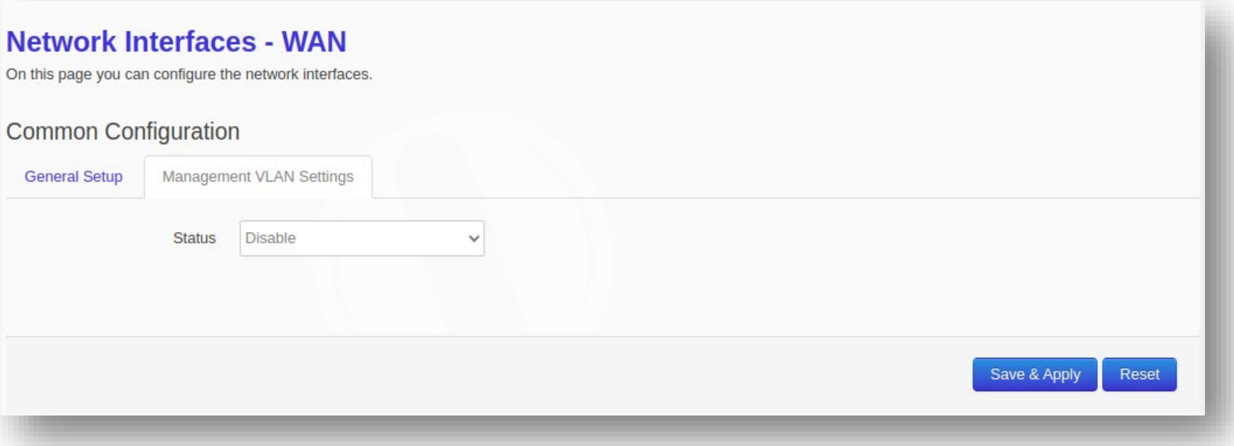
Dual Stack: Enable

Figure 25: General Setup Setting

S.No.	Field	Description
1.	Network Interface	Enables the users to configure network interfaces.
2.	Common Configuration	Gives the current configuration and enables users to re-configure them.
3.	General Setup	General configurations.
4.	Protocol	Protocol of the interface.
5.	Dual Stack	Enable/Disable dual stack of the interface.

Table 19: General Setup Description

5.5.1.1.2 Network Interface: Management VLAN Settings



Network Interfaces - WAN

On this page you can configure the network interfaces.

Common Configuration

Status: Disable

Figure 26: Management VLAN Setting

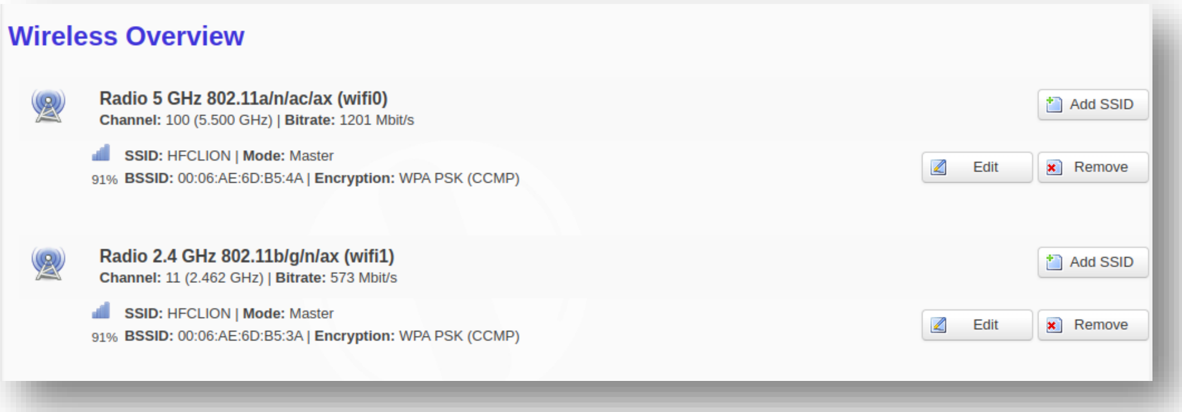
S.No.	Field	Description
1.	Network Interface	Enables the users to configure network interfaces.
2.	Common Configuration	Gives the current configuration and enables users to re-configure them.

3.	Management VLAN Settings	Configuration pertaining to Management VLAN settings.
4.	Status	Enable/Disable management VLAN.
5.	Save & Apply	All configuration changes made will be saved and applied.
6.	Reset	All configuration changes made but not saved will be discarded.

Table 20: Management VLAN Setting Description

5.5.2 Wireless

In this page, User can make changes in the existing configuration and can make new SSIDs of devices under the Radio bands.



Wireless Overview

Radio 5 GHz 802.11a/n/ac/ax (wifi0)
Channel: 100 (5.500 GHz) | **Bitrate:** 1201 Mbit/s

SSID: HFCLION | **Mode:** Master
91% **BSSID:** 00:06:AE:6D:B5:4A | **Encryption:** WPA PSK (CCMP)

Radio 2.4 GHz 802.11b/g/n/ax (wifi1)
Channel: 11 (2.462 GHz) | **Bitrate:** 573 Mbit/s

SSID: HFCLION | **Mode:** Master
91% **BSSID:** 00:06:AE:6D:B5:3A | **Encryption:** WPA PSK (CCMP)

Figure 27: Wireless Overview Screen

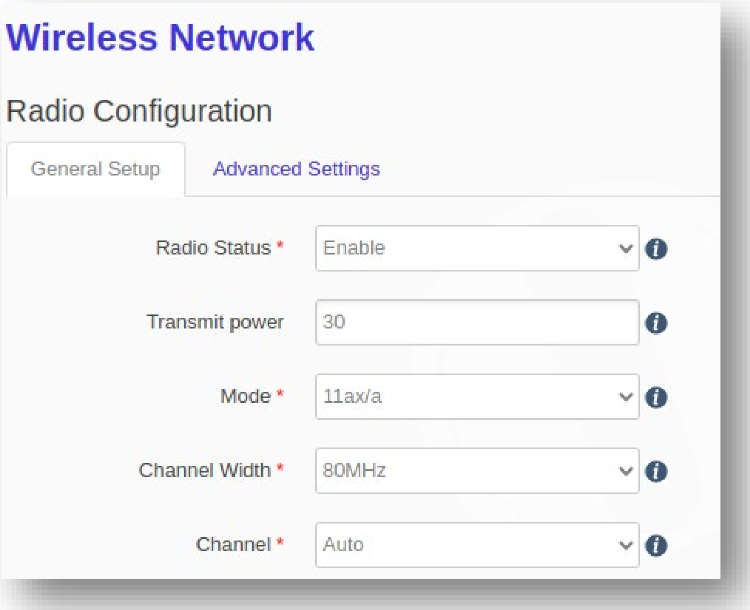
S.No.	Field	Description
1.	Wireless Overview	Allows the wireless settings to be configured as per user's requirement.
2.	Radio 2.4 GHz	Shows the SSIDs of Radio 2.4 GHz
3.	Radio 5GHz	Shows the SSIDs of Radio 5 GHz
4.	Add SSID	A new SSID can be added to the HMR device.
5.	Edit	Current configuration can be edited here.
6.	Remove	The specific SSID can be removed here.

Table 21: Wireless Description

- Detailed overview of wireless configurations are displayed for both Radio 2.4 GHz 802.11b/g/n/ax (wifi0) and Radio 5 GHz 802.11a/n/ac/ax (wifi1).
- Users can also make changes in the existing configuration and can also add new SSID of devices under the two radio bands: unlike the brief display of configuration under the System Tab of Dashboard. (Refer to Figure: 7 Wireless Summary Screen)
- On clicking **"Add SSID,"** user gets two sets of setting configuration
    - Radio Configuration
    - SSID Configuration

5.5.2.1.1 Add SSID

The user can add **SSID** by clicking on the **Add SSID** button for the radio.



Wireless Network

Radio Configuration

Radio Status * Enable

Transmit power 30

Mode * 11ax/a

Channel Width * 80MHz

Channel * Auto

Figure 28: Add SSID

S.No.	Field	Description
1.	Radio Status	Enable the radio status to make SSID visible to allow users to connect.
2.	Transmit power	Supported range from 6dBM to 23dBM.
3.	Mode	Wireless standard to be selected which is compatible with the device.
4.	Channel Width	Channel bandwidth in which radio needs to operate
5.	Channel	Selecting 'Auto' will automatically select one of the available channels.

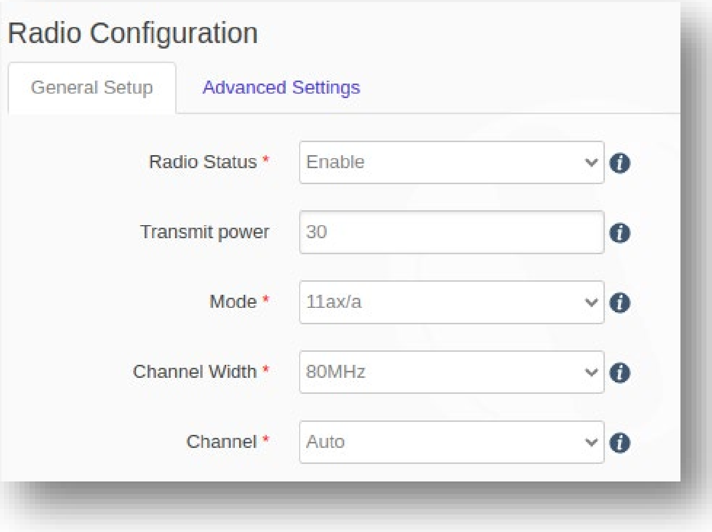
Table 22: Add SSID Description

5.5.2.2 Radio Configurations

In Radio Configurations settings, there are two sub-categories: General Settings & Advanced Settings

5.5.2.3 Radio Configuration: General Settings

- Radio Status
- Transmit power
- Mode
- Channel width
- Channel



Radio Configuration

Radio Status * Enable

Transmit power 30

Mode * 11ax/a

Channel Width * 80MHz

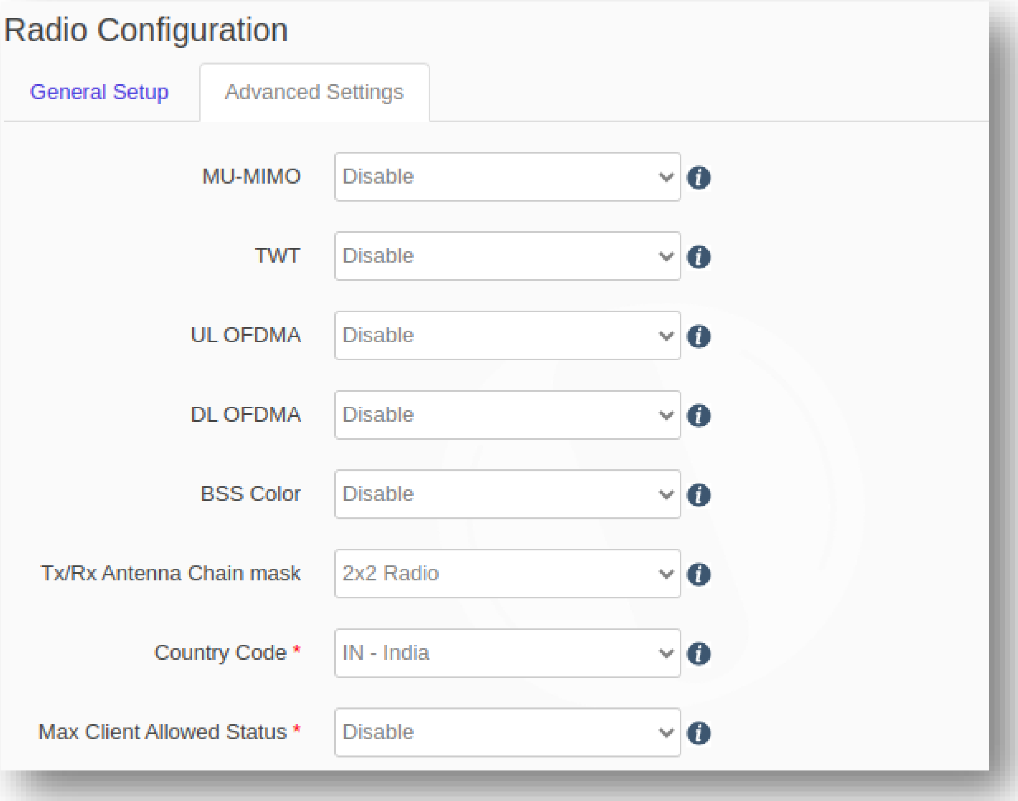
Channel * Auto

Figure 29: Radio Configuration General Settings

S.No.	Field	Description
1.	Wireless Network	Allows the wireless settings to be configured as per user's requirement.
2.	Radio Configuration	General Settings
3.	Radio Status	Enable the radio status to make SSID visible to allow users to connect.
4.	Transmit Power	Supported range from 6dBM to 23dBM.
5.	Mode	Wireless standard to be selected which is compatible with the device.
6.	Channel Width	Channel bandwidth in which radio needs to operate
7.	Channel	Selecting ‘Auto’ will automatically select one of the available channels.

Table 23: Radio Configuration General Settings Description

5.5.2.4 Radio Configuration: Advanced Settings



Radio Configuration

General Setup | Advanced Settings

MU-MIMO: Disable

TWT: Disable

UL OFDMA: Disable

DL OFDMA: Disable

BSS Color: Disable

Tx/Rx Antenna Chain mask: 2x2 Radio

Country Code *: IN - India

Max Client Allowed Status *: Disable

Figure 30: Radio Configuration Advanced Settings

S.No.	Field	Description
1.	Wireless Network	Allows the wireless settings to be configured as per user's requirement.
2.	Radio Configuration	Advanced Settings
3.	MU-MIMO	By enabling MU-MIMO, multiple clients connected to the access point will be able to send acknowledgement responses (ack) simultaneously, thus saving airtime. This ultimately improves network throughput and efficiency.
4.	TWT	It allows devices to negotiate when and how often they will wake up to send or receive data. TWT increases device sleep time and, in turn, substantially improves battery life.
5.	UL OFDMA	The total bandwidth is divided into several bundles of sub-carriers (denoted by resource units (RUs)) and each station transmits its UL frames through the allocated RU.
6.	DL OFDMA	The total bandwidth is divided into several bundles of sub-carriers (denoted by resource units (RUs)) and AP transmits its DL frames through the allocated RU.
7.	BSS Color	This helps mitigate overlapping Basic Service Sets (OBSS). In turn, this enables a network to more effectively – and concurrently – transmit data to multiple devices in congested areas.

8.	Tx/Rx Antenna Chain Mask	Users can select Tx/Rx Antenna Chain Mask 1x1 or 2x2.
9.	Country Code	Standard Country code.
10.	Max Client Allowed status	Enable Max Client Allowed to use Max Client Allowed

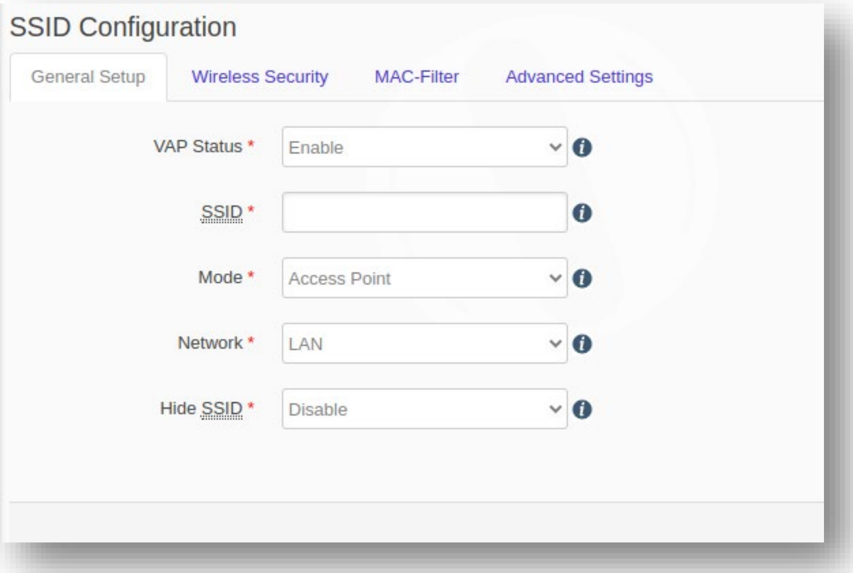
Table 24: Radio Configuration Advanced Settings

5.5.2.5 SSID Configurations

In the **SSID** Configuration page, user gets four further types of settings to configure SSIDs.

- General Setup
- Advanced Settings
- Wireless Security
- MAC Filter

5.5.2.5.1 SSID Configuration: General Settings



SSID Configuration

VAP Status * Enable

SSID *

Mode * Access Point

Network * LAN

Hide SSID * Disable

Figure 31: SSID Configuration General Settings

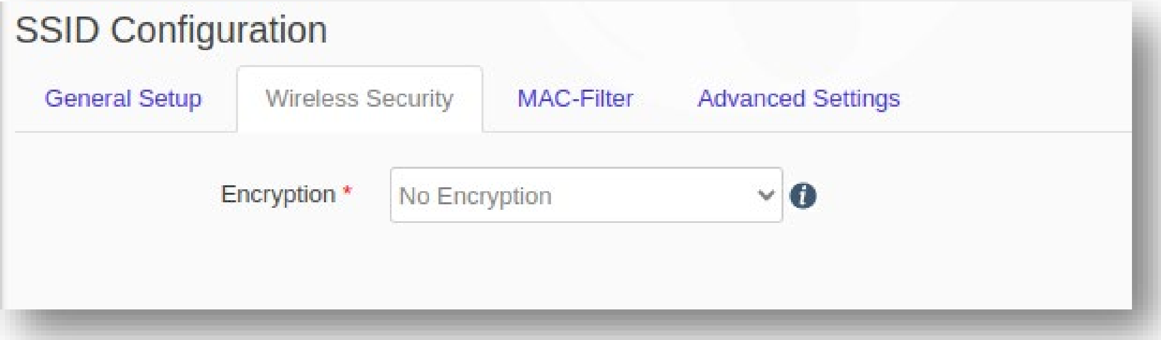
S.No.	Field	Description
1.	SSID Configuration	General Setup
2.	VAP Status	Select enable/disable to change the VAP status.
3.	SSID	Users can give the SSID of the device.
4.	Mode	In Access Point mode, Device can be connected to a wired network and transform the wired access into wireless that multiple devices can share together, especially for a home, office, or hotel where only wired network is available.
5.	Network	If DHCP Server is enabled, then the network will be NAT if DHCP Server is disabled then the network will be LAN.

6.	Hide SSID	Users can select enable/disable to change the Hide SSID status.

Table 25: SSID Configuration General Settings Description

5.5.2.5.2 SSID Configuration: Wireless Security

Users can choose the type of network authentication (data encryption) that is required to connect to the SSID.



SSID Configuration

Encryption * No Encryption

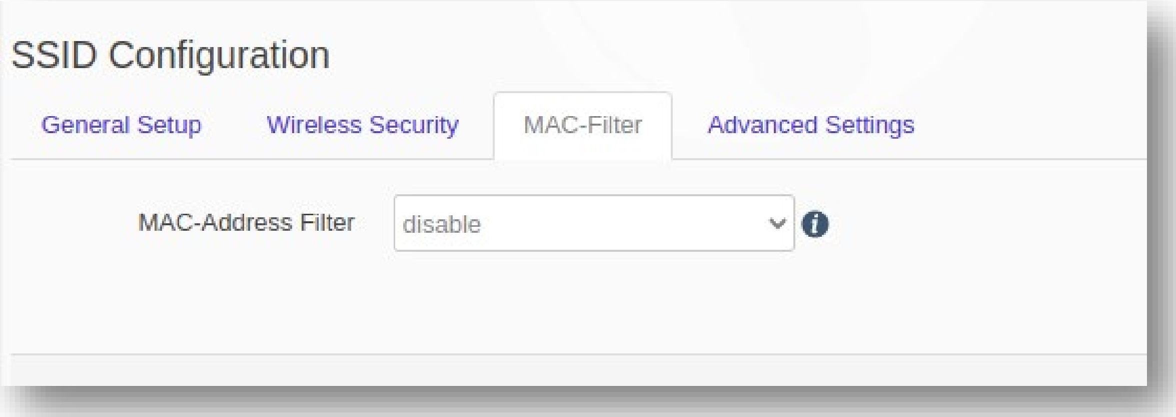
Figure 32: SSID Configuration Wireless Security

S.No.	Field	Description
1.	SSID Configuration	Wireless Security
2.	Encryption	Enables users to specify the encryption type to be set.

Table 26: SSID Configuration Wireless Security Description

5.5.2.5.3 SSID Configuration: MAC Filter

Users can select disable/Allow all listed/Allow all except listed.



SSID Configuration

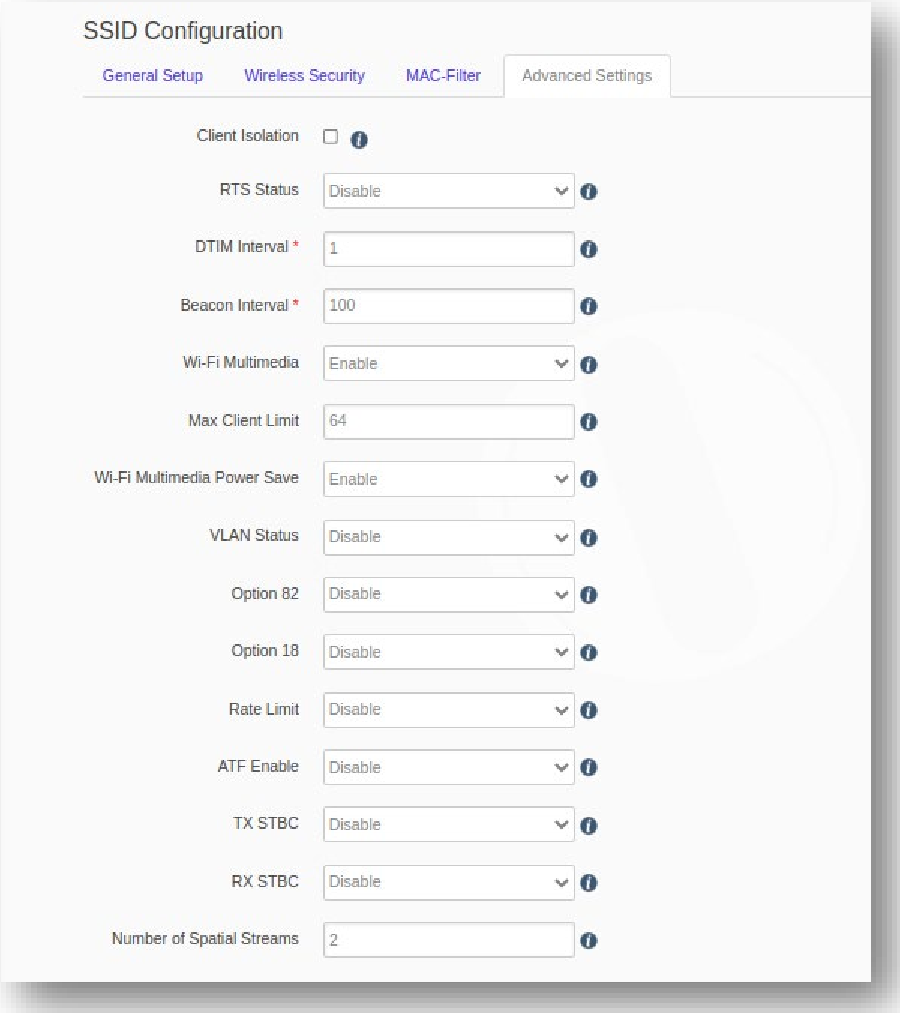
MAC-Address Filter disable

Figure 33: SSID Configuration MAC Filter

S.No.	Field	Description
1.	SSID Configuration	Mac Filter
2.	MAC-Address Filter	Can be enabled or disabled as per user requirements.

Table 27: SSID Configuration MAC Filter Description

5.5.2.5.4 SSID Configuration: Advanced Settings



SSID Configuration

Client Isolation □

RTS Status: Disable

DTIM Interval *: 1

Beacon Interval *: 100

Wi-Fi Multimedia: Enable

Max Client Limit: 64

Wi-Fi Multimedia Power Save: Enable

VLAN Status: Disable

Option 82: Disable

Option 18: Disable

Rate Limit: Disable

ATF Enable: Disable

TX STBC: Disable

RX STBC: Disable

Number of Spatial Streams: 2

Figure 34: SSID Configuration Advanced Setting

S.No.	Field	Description
1.	SSID Configuration	Advanced Settings
2.	Client Isolation	Prevents client-to-client communication
3.	RTS Status	Users can enable RTS Status to configure RTS.
4.	DTIM Interval	Specify the period of time to wake up clients from sleep mode to receive traffic at the right time. Allowed range is from 1ms to 255ms.
5.	Beacon Interval	Specify the time interval in which beacon packets have to be transmitted. Allowed range is from 100ms to 300ms.
6.	Wi-Fi Multimedia	Enabling the WMM will control the upstream traffic flow from Wi-Fi device to AP and downstream traffic flow from AP to Wi-Fi device.
7.	Max Client Limit	Supported range from 1-128.
8.	Wi-Fi multimedia Power Save	WMM-Power Save increases the efficiency and flexibility of data transmission. Specifically, the client device can doze between packets to save power, while the access point buffers downlink

		frames. The application chooses the time to wake up and receive data packets to maximize power conservation without sacrificing Quality of Service.
9.	VLAN Status	VLAN status enable/disable, if VLAN will be enabled then VLAN value 1 will be set by default.
10.	Option 82	This will add client VLAN ID in Option82 field (IPv4).
11.	Option 18	This will add client VLAN ID in Option18 field (IPv6).
12.	Rate Limit	Enable Rate Limit per VAP or Rate Limit per Client to select Upload Limit and Download Limit.
13.	ATF Enable	Enable ATF to use ATF feature.
14.	TX STBC	Space time block coding (STBC) transmits multiple copies of one data flow in wireless communication. STBC uses many antennas to produce multiple receive versions of data, improving data transmission reliability.
15.	Number of spatial streams	Spatial Streams 1-2 is supported.

Table 28: Radio Configuration Advanced Settings Description

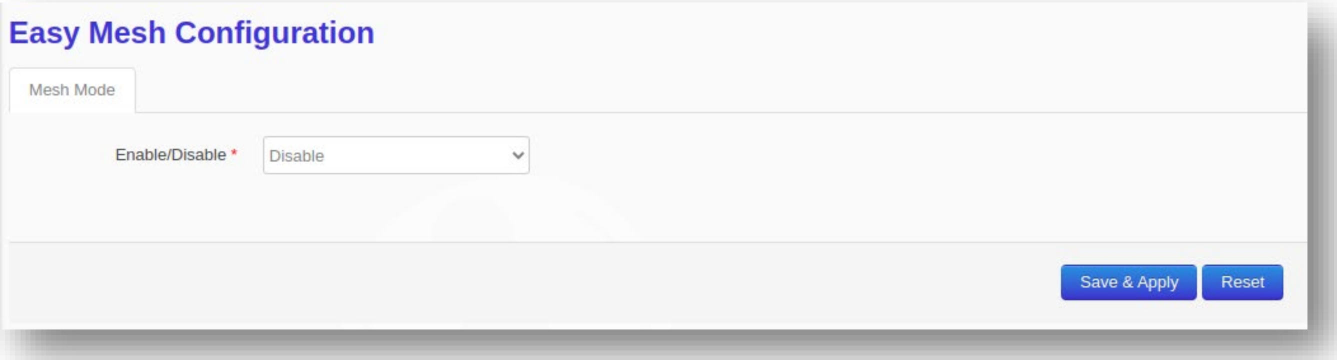
5.5.3 Easy Mesh Configuration

A wireless mesh network serves as a network of radio nodes organized in a mesh topology. All APs participating in mesh topology does not need to have a wired connection for backhaul connectivity and only one root AP serves that purpose.

Mesh configurations require access points to operate in two operating modes as follows:

- Controller AP: Controller AP have wired connections, for example, Ethernet backhaul to a wired network and to cNMS.
- Agent AP: Repeats wireless signals to extend range without being connected with cable to Access Point, or with clients.

Mesh configuration allows access points to connect with each other in mesh topology. An access point (Controller AP) is connected to the wired network with the use of wireless connections over the 802.11 radio backhaul and other agent access points act as repeaters in mesh topology. In case of a mesh node failure, the surrounding nodes automatically re-connect and resume service without downtime. Nodes identify the best next hop and connect with it automatically.



Easy Mesh Configuration

Mesh Mode

Enable/Disable * Disable

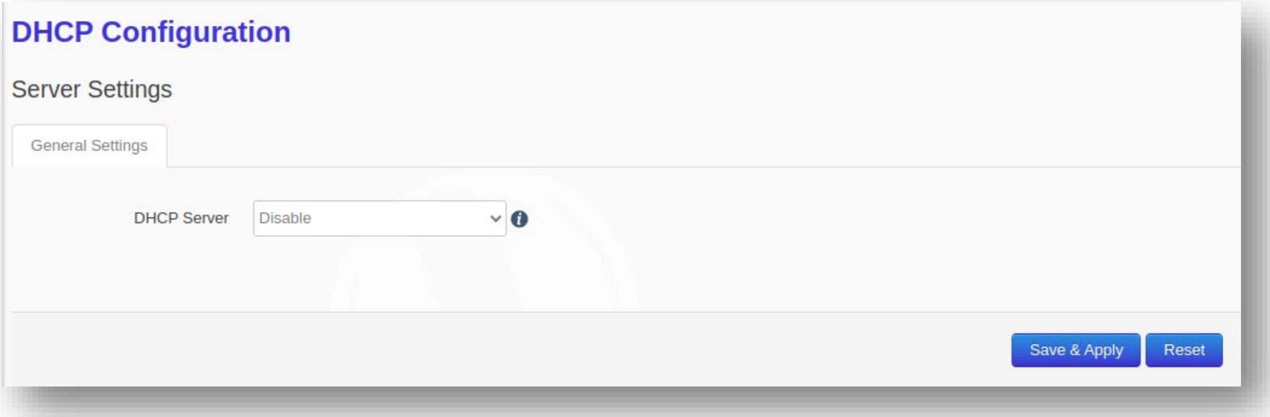
Figure 35: Easy Mesh Configuration

S.No.	Field	Description
1.	Easy Mesh Configuration	Users can configure easy mesh configuration.
2.	Enable/Disable	Mesh mode can be enabled/disabled.
3.	AP Mode	AP Mode to be selected
4.	Agent Mode	Agent Mode to be configured.
5.	WPS	Enable Wi-Fi-protected setup by choosing either soft or hard WPS (software or hardware respectively).

Table 29: Easy Mesh Configuration Description

5.5.4 DHCP Server Configuration

The AP itself can act as a DHCP service provider for the connected clients and configuration for the same is executed from this screen. A basic overview of the screen to enable thick AP as DHCP server (IPv4) is given below:



DHCP Configuration

Server Settings

General Settings

DHCP Server: Disable

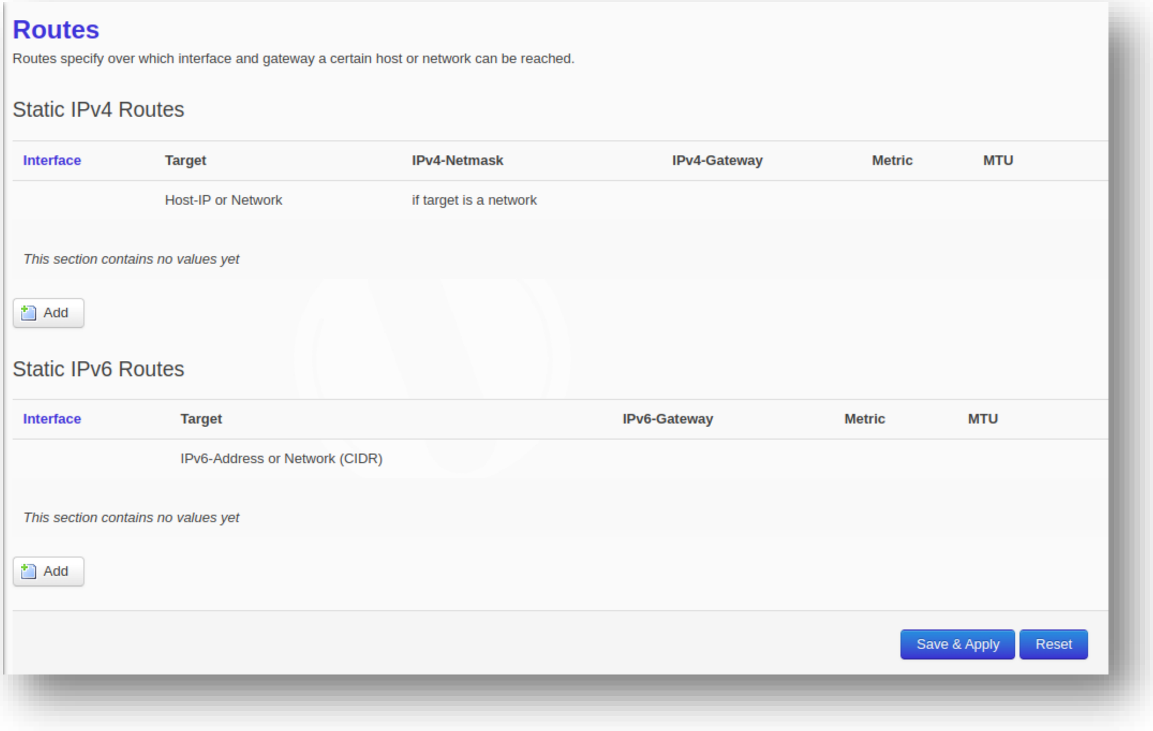
Figure 36: DHCP Configuration

S.No.	Field	Description
1.	DHCP Configuration	DHCP protocol settings can be configured as per user requirements.
2.	Server Settings	DHCP server settings can be configured.
3.	DHCP Server	Can be enabled/disabled.

Table 30: DHCP Configuration Description

5.5.5 Static Routes

Users can specify the interface and gateway through which a certain host or network can be reached in the Route Configuration tab. Both static IPv4 and static IPv6 routes can be configured by the user. Before clicking the **Add** Button, the page looks like:



Routes

Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	MTU
	Host-IP or Network	if target is a network			

This section contains no values yet

Static IPv6 Routes

Interface	Target	IPv6-Gateway	Metric	MTU
	IPv6-Address or Network (CIDR)			

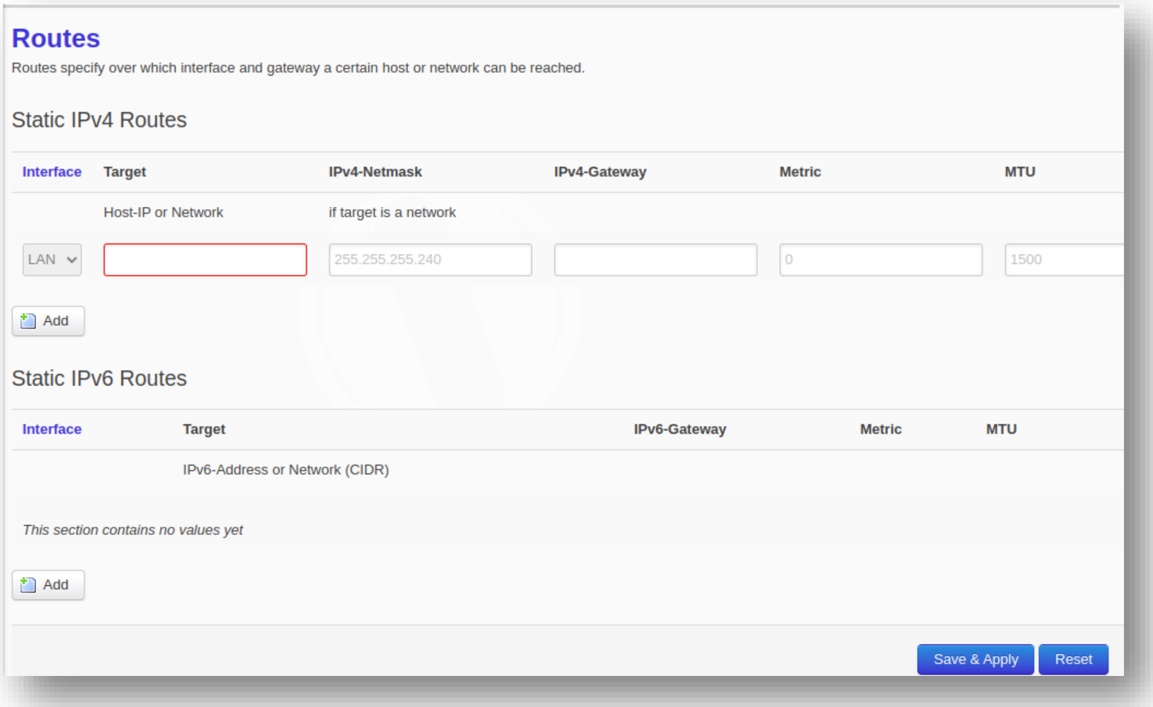
This section contains no values yet

Figure 37: Static Routes (1)

S.No.	Field	Description
1.	Routes	Specifies over which interface and gateway a certain host or network can be reached.
2.	Static IPv4 Routes	All static IPv4 routes are displayed
3.	Add	New static IPv4 routes can be added by the end-user.
4.	Static IPv6 Routes	All static IPv6 routes are displayed.
5.	Add	New static IPv6 routes can be added by the end-user.

Table 31: Static Routes_1 Description

After clicking **Add** Button, the page looks like:



Routes

Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	MTU
	Host-IP or Network	if target is a network			
LAN		255.255.255.240		0	1500

Add

Static IPv6 Routes

Interface	Target	IPv6-Gateway	Metric	MTU
	IPv6-Address or Network (CIDR)			

This section contains no values yet

Add

Save & Apply Reset

Figure 38: Static Routes_2

S.No.	Field	Description
1.	Routes	Specifies over which interface and gateway a certain host or network can be reached.
2.	Static IPv4 Routes	New static IPv4 routes are added.
3.	Interface	Interface, along with the Host-IP, IPv4 target, gateway and MTU can be configured by the end-user.
4.	Static IPv6 Routes	New static IPv6 routes are added.
5.	Interface	Interface, along with the Host-IP, IPv6 target, gateway and MTU can be configured by the end-user.
6.	Add	More routes can be added as required.
7.	Save & Apply	All new configuration changes will be applied after being saved.
8.	Reset	All configuration changes which have not been saved and applied will be discarded.

Table 32: Static Routes_2 Description

5.6 Wi-Fi Schedule

Wi-Fi schedules can be created and viewed by the user as per their own configurations. It has two categories: **Create Schedule & View Schedule.**

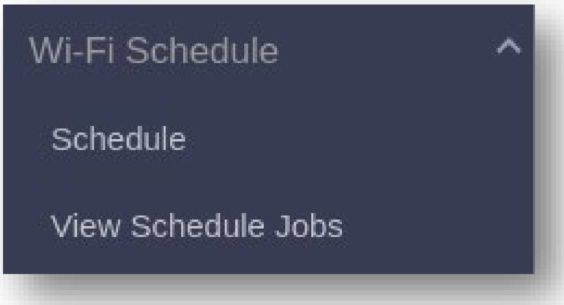
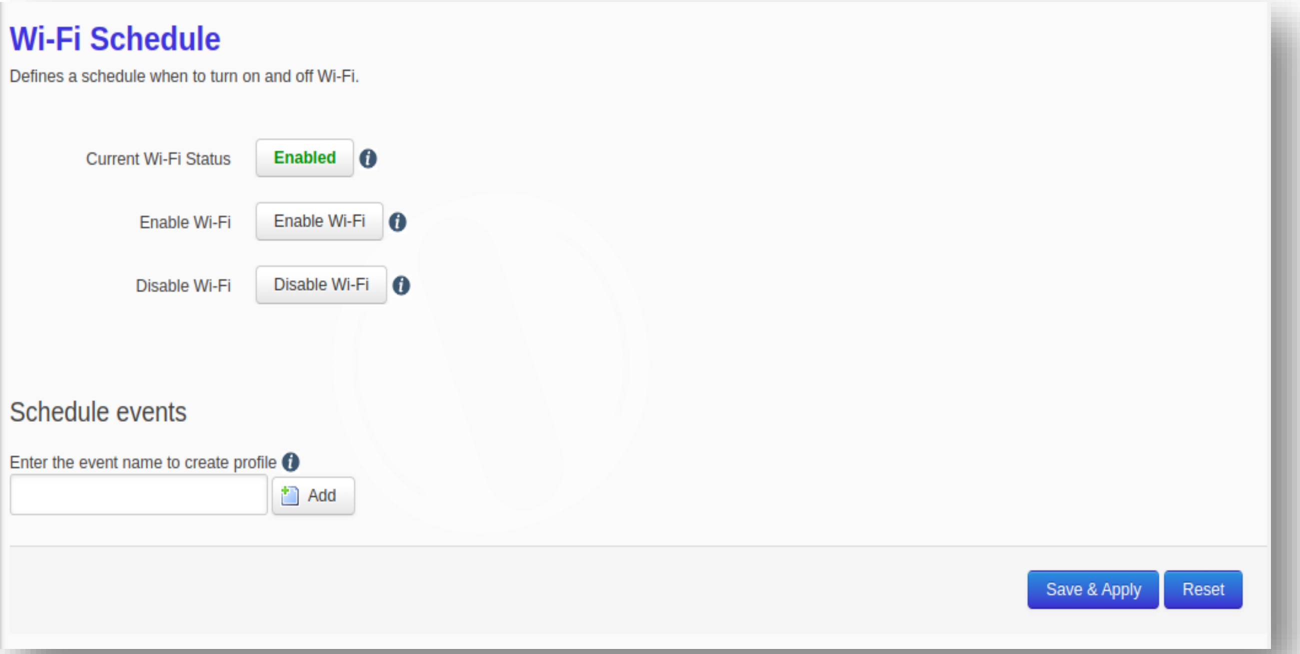


Figure 39: Wi-Fi Schedule


Wi-Fi Schedule

Defines a schedule when to turn on and off Wi-Fi.

Current Wi-Fi Status: Enabled

Schedule events

Enter the event name to create profile

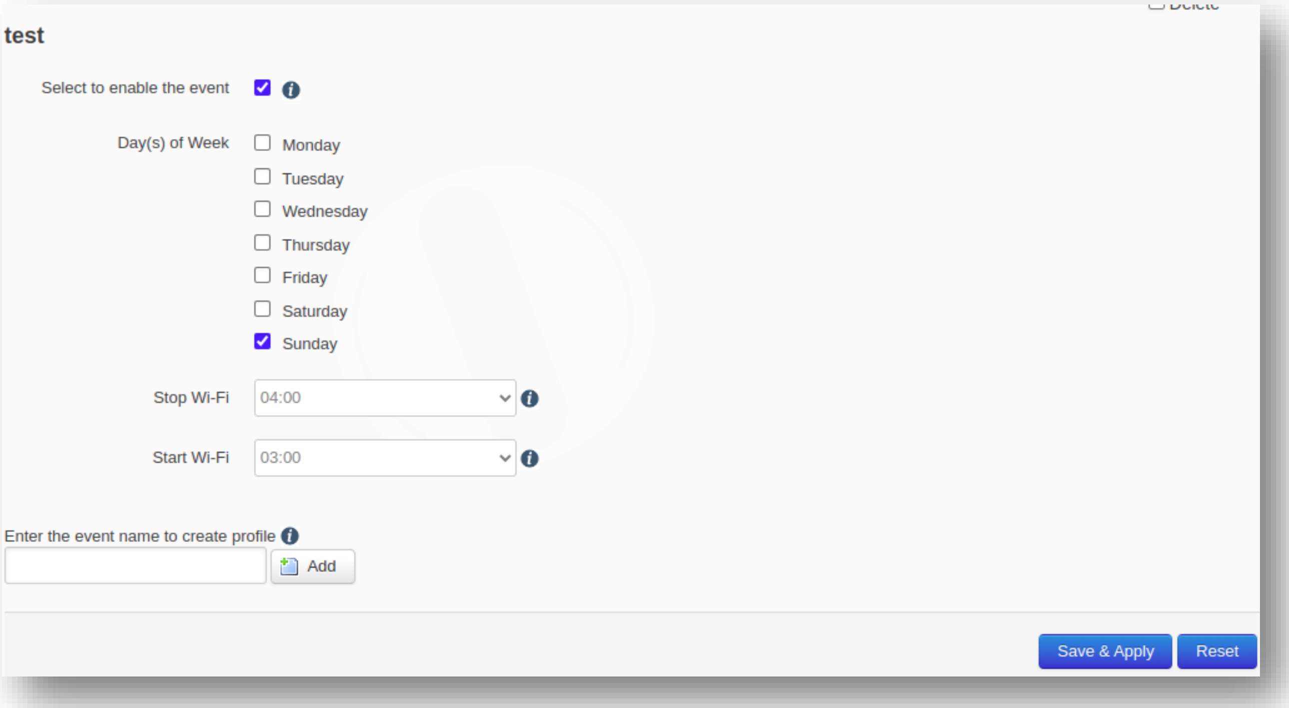
Figure 40: Wi-Fi Schedule

S.No.	Field	Description
1.	Wi-Fi Schedule	Wi-fi schedule can be configured by the end-users.
2.	Current Wi-fi Status	Can configure the current wi-fi status (enables/ disabled)
3.	Schedule Events	Event name to create profile.
4.	Add	To add a schedule event.
5.	Save and Apply	Changes will be applied after saving.
6.	Reset	All changes not saved and applied will be discarded.
7.	Unsaved Changes	All changes unsaved for configuration.

Table 33: Wi-Fi Schedule Description

5.6.1 Create Schedule

The current status of the Wi-Fi on the AP is displayed. The user can enter the Wi-Fi Schedule profile name. This profile name should not be the same as an existing profile name. This is not case sensitive.



test

Select to enable the event ☑

Day(s) of Week
- □ Monday
- □ Tuesday
- □ Wednesday
- □ Thursday
- □ Friday
- □ Saturday
- ☑ Sunday

Stop Wi-Fi 04:00

Start Wi-Fi 03:00

Enter the event name to create profile

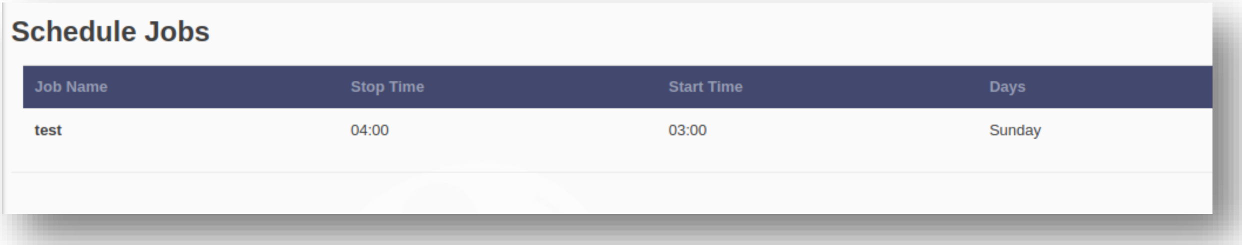
Figure 41: Create Wi-Fi Schedule

S.No.	Field	Description
1.	Select to enable the event	If selected, the user can schedule the event
2.	Days of Week	Select the days for event
3.	Stop Wi-Fi	Select the Wi-Fi stop time
4.	Start Wi-Fi	Select the Wi-Fi start time
5.	Add	Enter the event name to create profile
6.	Save and Apply	Changes will be applied after saving.
7.	Reset	All changes not saved and applied will be discarded.
8.	Unsaved Changes	All changes unsaved for configuration.

Table 34: Create Wi-Fi Schedule Description

5.6.2 View Schedule

Any schedule created will be populated on the screen under the 'View Schedule' Tab.



Schedule Jobs

Job Name	Stop Time	Start Time	Days
test	04:00	03:00	Sunday

Figure 42: View Wi-Fi Schedule

S.No.	Field	Description
1.	View Schedule	Any schedule created will be displayed.
2.	Job Name	The name of job schedule.
3.	Stop Time	Time at which the schedule will stop.
4.	Start Time	Time at which the schedule will start.
5.	Days	Days the job schedule will be run.
6.	Unsaved Changes	Any changes unsaved.

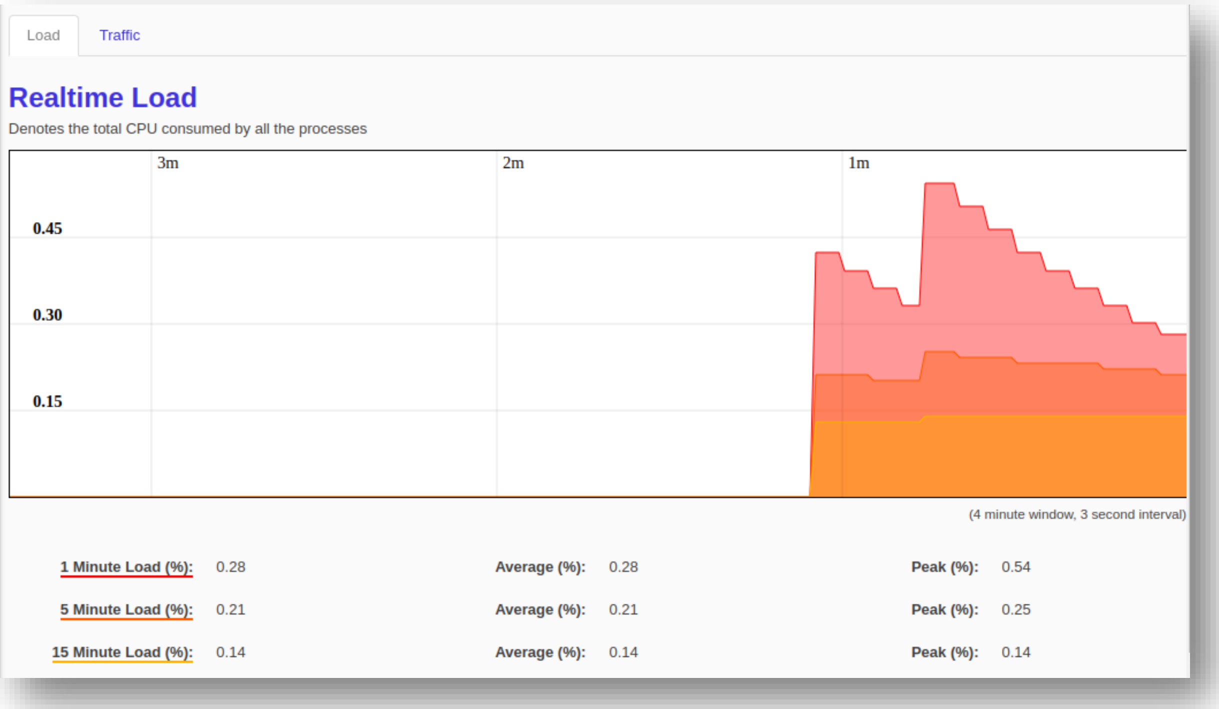
Table 35: View Wi-Fi Schedule Description

5.7 Statistics

All statistical information such as reports, and statistical graphs will be rendered to the user. It includes Realtime Graphs & Reports.

5.7.1 Realtime Graphs

The real time load graph shows the CPU load of the last 3 min and the graph is refreshed at every 3 sec intervals. In addition to the displayed graph the user can find the average and the peak CPU load values of the respective AP. A basic overview of the Real-time load graphs screen is given below:



Realtime Load

Denotes the total CPU consumed by all the processes

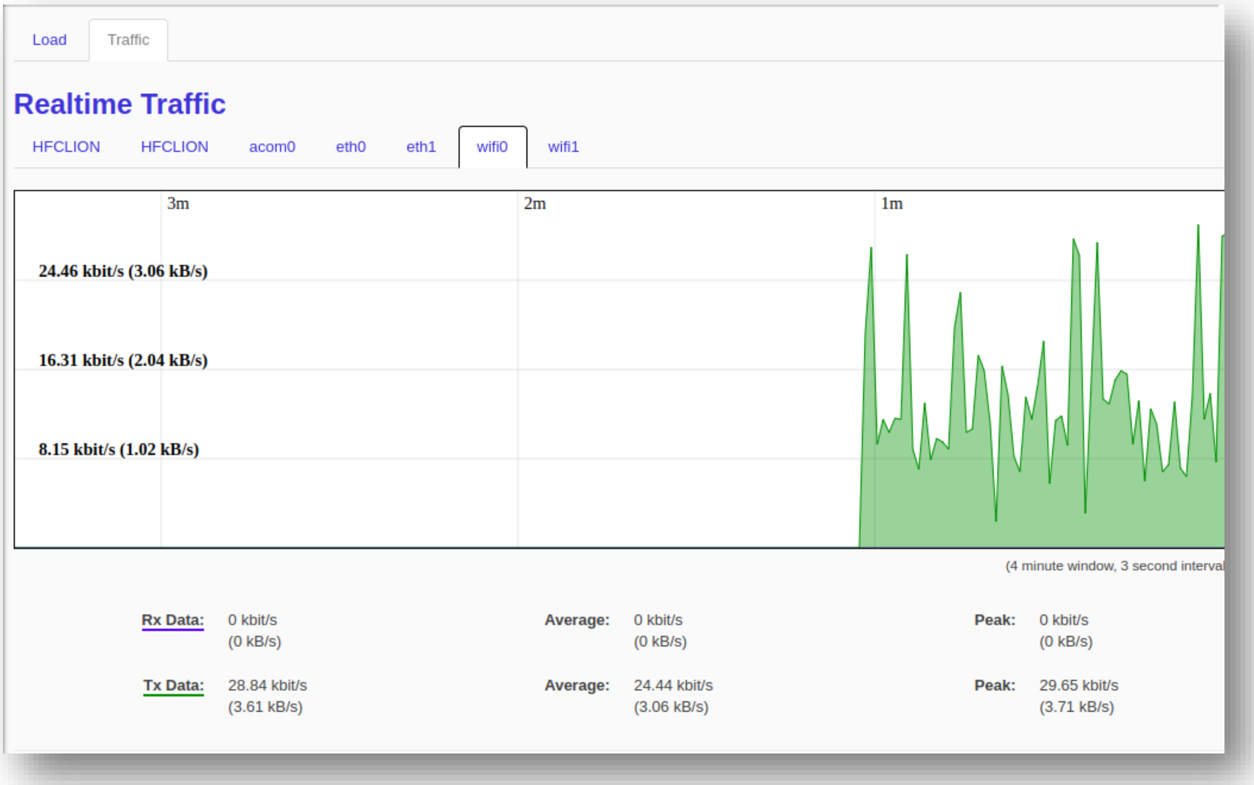
(4 minute window, 3 second interval)

1 Minute Load (%):	0.28	Average (%):	0.28	Peak (%):	0.54
5 Minute Load (%):	0.21	Average (%):	0.21	Peak (%):	0.25
15 Minute Load (%):	0.14	Average (%):	0.14	Peak (%):	0.14

Figure 43: Real Time Load

S.No.	Field	Description
1.	Statistics	Statistical information is rendered on this page.
2.	Realtime Traffic	Real time traffic is rendered to end-users in the form of graphs.
3.	Realtime Load	Real time load is depicted by the total CPU consumed by all the processes.

Table 36: Realtime Load Description



Realtime Traffic

Rx Data:	0 kbit/s (0 kB/s)	Average:	0 kbit/s (0 kB/s)	Peak:	0 kbit/s (0 kB/s)
Tx Data:	28.84 kbit/s (3.61 kB/s)	Average:	24.44 kbit/s (3.06 kB/s)	Peak:	29.65 kbit/s (3.71 kB/s)

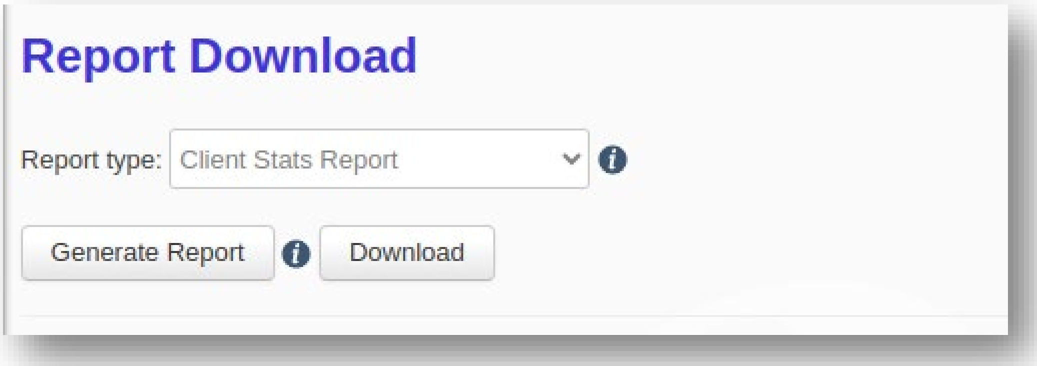
Figure 44: Real Time Traffic

S.No.	Field	Description
1.	Statistics	Statistical information is rendered on this page.
2.	Realtime Graphs	All real time graphs pertaining to different fields are rendered.
3.	Realtime Traffic	All real time traffic pertaining to different fields are rendered.

Table 37: Realtime Traffic Description

5.8 Reports

All the reports generated by the user can be downloaded for their perusal.



Report Download

Report type: Client Stats Report

Figure 45: Report

S.No.	Field	Description
1.	Report Download	Reports can be downloaded by end-users in tar format for their perusal.
2.	Report Type	Report type can be selected as required.
3.	Generate Report	Reports are generated and automatically downloaded.

Table 38: Reports Description

5.9 Diagnostics

All the diagnostics services will be rendered to the user:

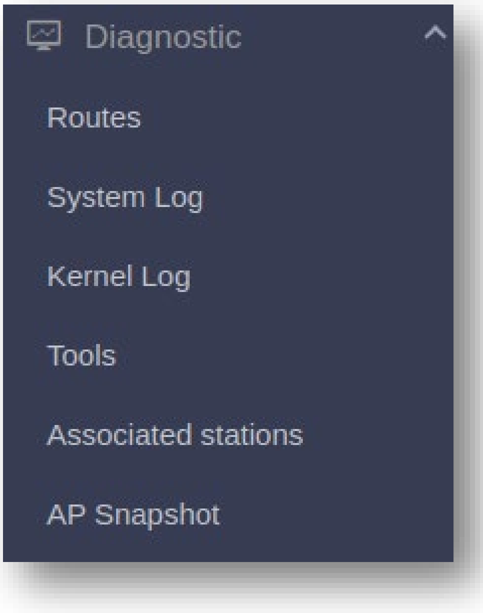
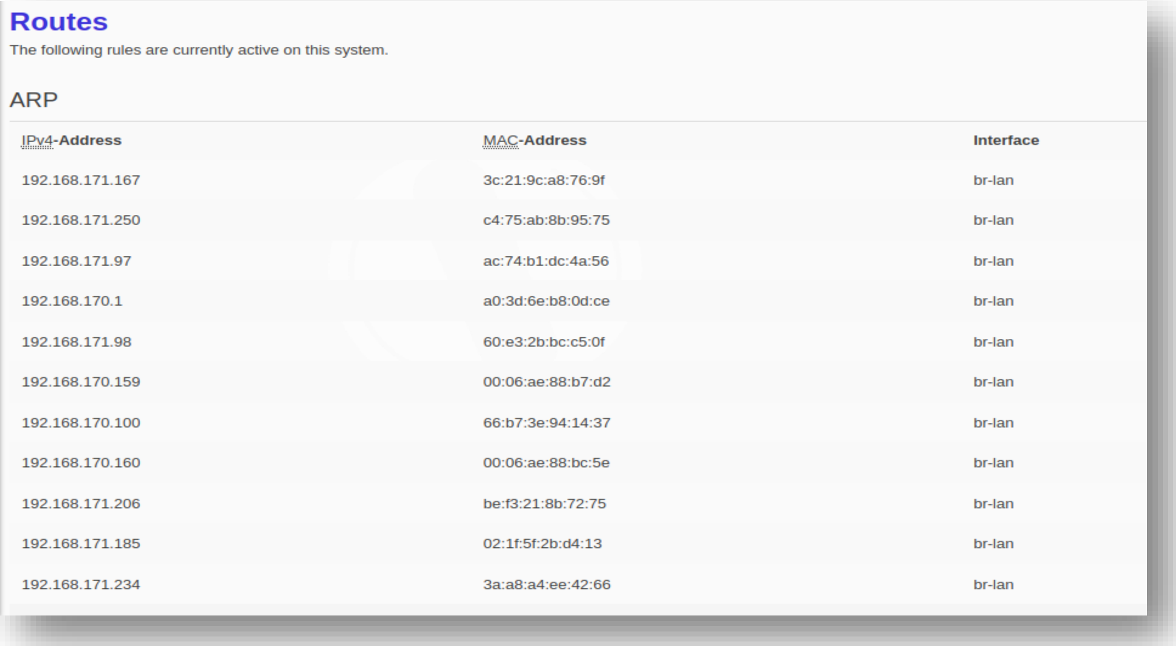


Figure 46: Diagnostics

- Routes
- System Log
- Kernel Log
- Tools
- Associated stations
- AP snapshots

5.9.1 Routes



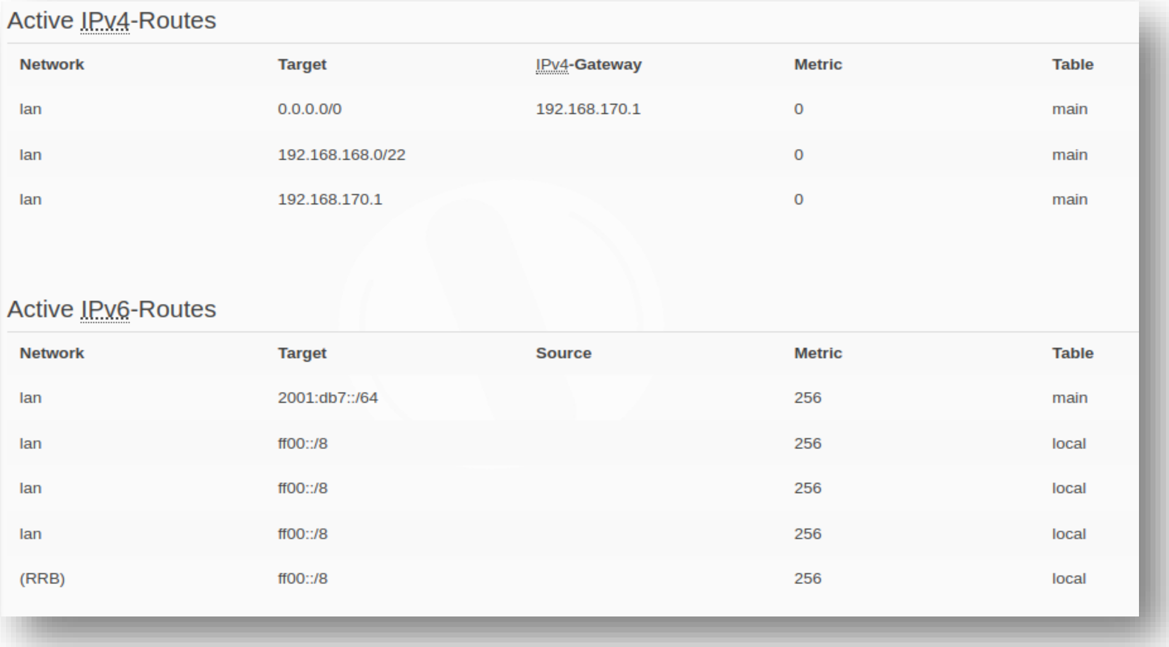
Routes

The following rules are currently active on this system.

ARP

IPv4-Address	MAC-Address	Interface
192.168.171.167	3c:21:9c:a8:76:9f	br-lan
192.168.171.250	c4:75:ab:8b:95:75	br-lan
192.168.171.97	ac:74:b1:dc:4a:56	br-lan
192.168.170.1	a0:3d:6e:b8:0d:ce	br-lan
192.168.171.98	60:e3:2b:bc:c5:0f	br-lan
192.168.170.159	00:06:ae:88:b7:d2	br-lan
192.168.170.100	66:b7:3e:94:14:37	br-lan
192.168.170.160	00:06:ae:88:bc:5e	br-lan
192.168.171.206	be:f3:21:8b:72:75	br-lan
192.168.171.185	02:1f:5f:2b:d4:13	br-lan
192.168.171.234	3a:a8:a4:ee:42:66	br-lan

Figure 47: Routes Tab



Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric	Table
lan	0.0.0.0/0	192.168.170.1	0	main
lan	192.168.168.0/22		0	main
lan	192.168.170.1		0	main

Active IPv6-Routes

Network	Target	Source	Metric	Table
lan	2001:db7::/64		256	main
lan	ff00::/8		256	local
lan	ff00::/8		256	local
lan	ff00::/8		256	local
(RRB)	ff00::/8		256	local

Figure 48: Active IPv4/IPv6 Routes

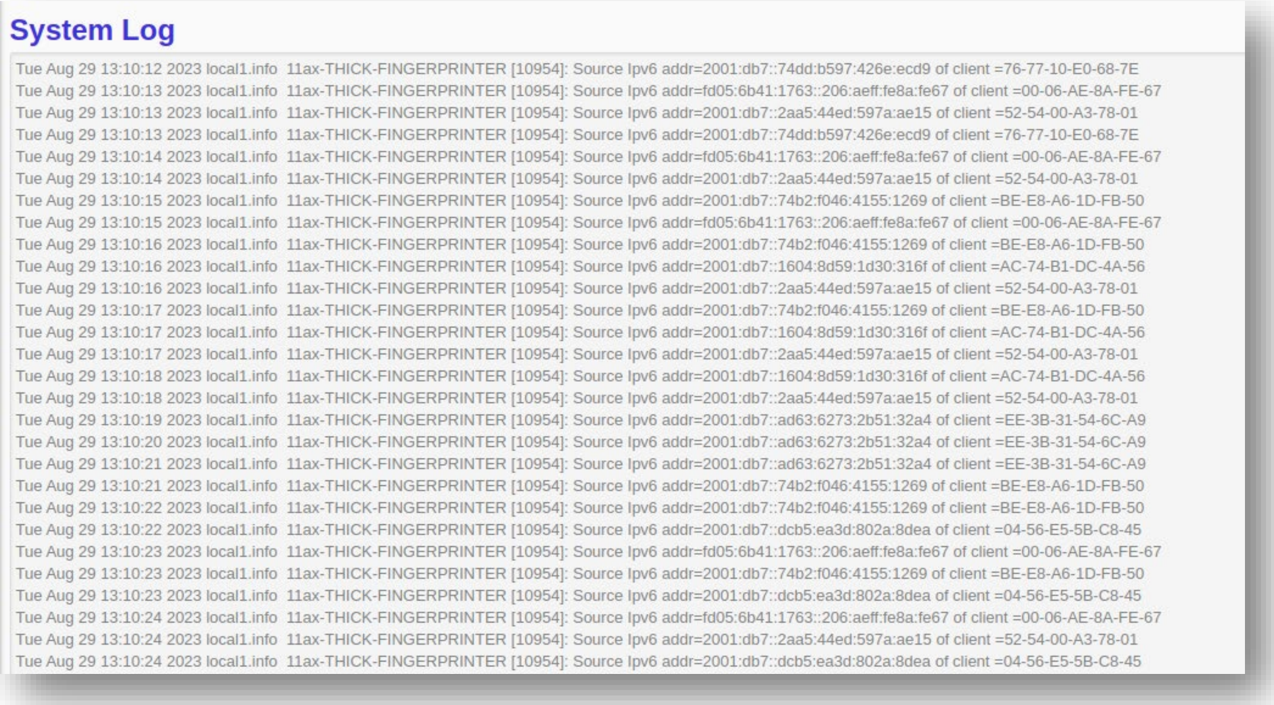
S.No.	Field	Description
1.	Routes	Routing routes are rendered for end-users.
2.	ARP	Address Resolution Protocol are displayed.
3.	Active IPv4 Routes	Current configured active IPv4 routes are displayed.
4.	Active IPv6 Routes	Current configured active IPv6 routes are displayed.

Table 39: Routes Description

5.9.2 System Log

This screen is provided to view the AP logs if the user faces any issue or wants to view the back-end logs. Only new logs are shown in this screen. However, old logs are stored in the database but will not be shown in this screen.

A basic overview of the System Log screen is given below:



System Log

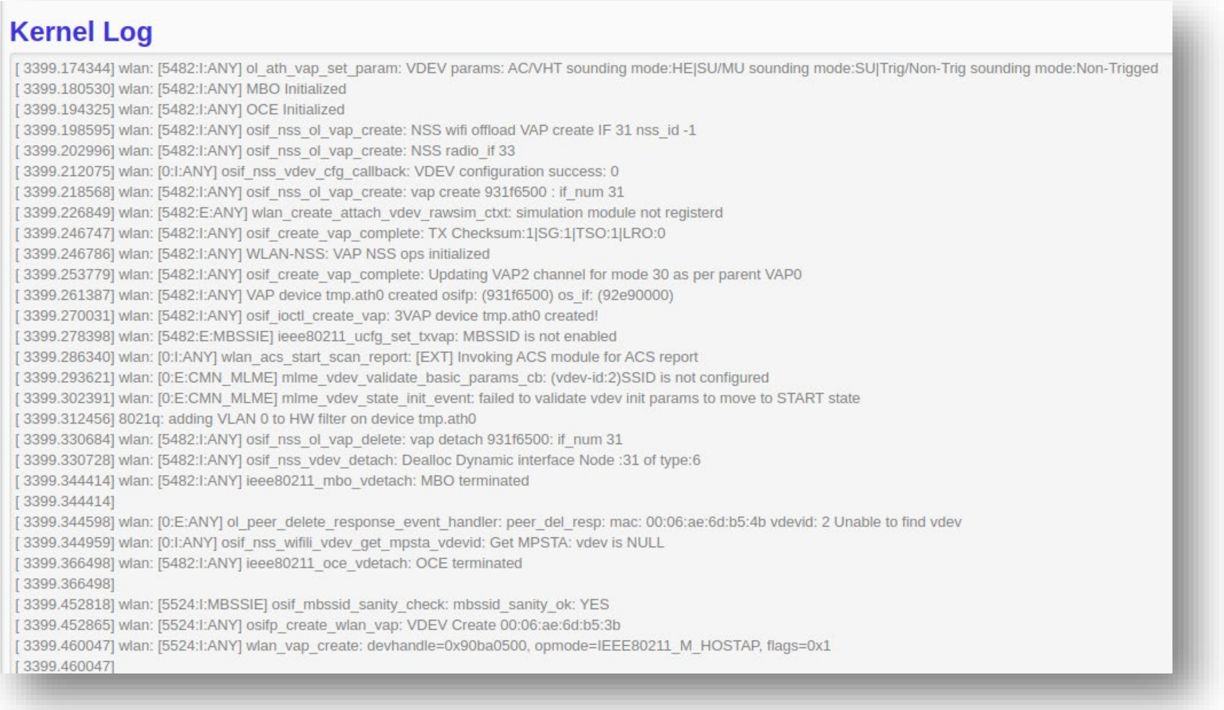
```
Tue Aug 29 13:10:12 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::74dd:b597:426e:ecd9 of client =76-77-10-E0-68-7E
Tue Aug 29 13:10:13 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=fd05:6b41:1763::206:aeff:fe8a:fe67 of client =00-06-AE-8A-FE-67
Tue Aug 29 13:10:13 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::2aa5:44ed:597a:ae15 of client =52-54-00-A3-78-01
Tue Aug 29 13:10:13 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::74dd:b597:426e:ecd9 of client =76-77-10-E0-68-7E
Tue Aug 29 13:10:14 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=fd05:6b41:1763::206:aeff:fe8a:fe67 of client =00-06-AE-8A-FE-67
Tue Aug 29 13:10:14 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::2aa5:44ed:597a:ae15 of client =52-54-00-A3-78-01
Tue Aug 29 13:10:15 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::74b2:f046:4155:1269 of client =BE-E8-A6-1D-FB-50
Tue Aug 29 13:10:15 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=fd05:6b41:1763::206:aeff:fe8a:fe67 of client =00-06-AE-8A-FE-67
Tue Aug 29 13:10:16 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::74b2:f046:4155:1269 of client =BE-E8-A6-1D-FB-50
Tue Aug 29 13:10:16 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::1604:8d59:1d30:316f of client =AC-74-B1-DC-4A-56
Tue Aug 29 13:10:16 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::2aa5:44ed:597a:ae15 of client =52-54-00-A3-78-01
Tue Aug 29 13:10:17 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::74b2:f046:4155:1269 of client =BE-E8-A6-1D-FB-50
Tue Aug 29 13:10:17 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::1604:8d59:1d30:316f of client =AC-74-B1-DC-4A-56
Tue Aug 29 13:10:17 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::2aa5:44ed:597a:ae15 of client =52-54-00-A3-78-01
Tue Aug 29 13:10:18 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::1604:8d59:1d30:316f of client =AC-74-B1-DC-4A-56
Tue Aug 29 13:10:18 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::2aa5:44ed:597a:ae15 of client =52-54-00-A3-78-01
Tue Aug 29 13:10:19 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::ad63:6273:2b51:32a4 of client =EE-3B-31-54-6C-A9
Tue Aug 29 13:10:20 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::ad63:6273:2b51:32a4 of client =EE-3B-31-54-6C-A9
Tue Aug 29 13:10:21 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::ad63:6273:2b51:32a4 of client =EE-3B-31-54-6C-A9
Tue Aug 29 13:10:21 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::74b2:f046:4155:1269 of client =BE-E8-A6-1D-FB-50
Tue Aug 29 13:10:22 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::74b2:f046:4155:1269 of client =BE-E8-A6-1D-FB-50
Tue Aug 29 13:10:22 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::dcb5:ea3d:802a:8dea of client =04-56-E5-5B-C8-45
Tue Aug 29 13:10:23 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=fd05:6b41:1763::206:aeff:fe8a:fe67 of client =00-06-AE-8A-FE-67
Tue Aug 29 13:10:23 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::74b2:f046:4155:1269 of client =BE-E8-A6-1D-FB-50
Tue Aug 29 13:10:23 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::dcb5:ea3d:802a:8dea of client =04-56-E5-5B-C8-45
Tue Aug 29 13:10:24 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=fd05:6b41:1763::206:aeff:fe8a:fe67 of client =00-06-AE-8A-FE-67
Tue Aug 29 13:10:24 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::2aa5:44ed:597a:ae15 of client =52-54-00-A3-78-01
Tue Aug 29 13:10:24 2023 local1.info  11ax-THICK-FINGERPRINTER [10954]: Source Ipv6 addr=2001:db7::dcb5:ea3d:802a:8dea of client =04-56-E5-5B-C8-45
```

Figure 49: System Log

S.No.	Field	Description
1.	System Log	System specific logs are rendered to the end-users.

Table 40: System Log Description

5.9.3 Kernel Log



```
[ 3399.174344] wlan: [5482:I:ANY] ol_ath_vap_set_param: VDEV params: AC/VHT sounding mode:HE|SU/MU sounding mode:SU|Trig/Non-Trig sounding mode:Non-Trigged
[ 3399.180530] wlan: [5482:I:ANY] MBO Initialized
[ 3399.194325] wlan: [5482:I:ANY] OCE Initialized
[ 3399.198595] wlan: [5482:I:ANY] osif_nss_ol_vap_create: NSS wifi offload VAP create IF 31 nss_id -1
[ 3399.202996] wlan: [5482:I:ANY] osif_nss_ol_vap_create: NSS radio_if 33
[ 3399.212075] wlan: [0:I:ANY] osif_nss_vdev_cfg_callback: VDEV configuration success: 0
[ 3399.218568] wlan: [5482:I:ANY] osif_nss_ol_vap_create: vap create 931f6500 : if_num 31
[ 3399.226849] wlan: [5482:E:ANY] wlan_create_attach_vdev_rawsim_ctxt: simulation module not registerd
[ 3399.246747] wlan: [5482:I:ANY] osif_create_vap_complete: TX Checksum:1|SG:1|TSO:1|LRO:0
[ 3399.246786] wlan: [5482:I:ANY] WLAN-NSS: VAP NSS ops initialized
[ 3399.253779] wlan: [5482:I:ANY] osif_create_vap_complete: Updating VAP2 channel for mode 30 as per parent VAP0
[ 3399.261387] wlan: [5482:I:ANY] VAP device tmp.ath0 created osifp: (931f6500) os_if: (92e90000)
[ 3399.270031] wlan: [5482:I:ANY] osif_ioctl_create_vap: 3VAP device tmp.ath0 created!
[ 3399.278398] wlan: [5482:E:MBSSIE] ieee80211_ucfg_set_txvap: MBSSID is not enabled
[ 3399.286340] wlan: [0:I:ANY] wlan_acs_start_scan_report: [EXT] Invoking ACS module for ACS report
[ 3399.293621] wlan: [0:E:CMN_MLME] mlme_vdev_validate_basic_params_cb: (vdev-id:2)SSID is not configured
[ 3399.302391] wlan: [0:E:CMN_MLME] mlme_vdev_state_init_event: failed to validate vdev init params to move to START state
[ 3399.312456] 8021q: adding VLAN 0 to HW filter on device tmp.ath0
[ 3399.330684] wlan: [5482:I:ANY] osif_nss_ol_vap_delete: vap detach 931f6500: if_num 31
[ 3399.330728] wlan: [5482:I:ANY] osif_nss_vdev_detach: Dealloc Dynamic interface Node :31 of type:6
[ 3399.344414] wlan: [5482:I:ANY] ieee80211_mbo_vdetach: MBO terminated
[ 3399.344414]
[ 3399.344598] wlan: [0:E:ANY] ol_peer_delete_response_event_handler: peer_del_resp: mac: 00:06:ae:6d:b5:4b vdevid: 2 Unable to find vdev
[ 3399.344959] wlan: [0:I:ANY] osif_nss_wifili_vdev_get_mpsta_vdevid: Get MPSTA: vdev is NULL
[ 3399.366498] wlan: [5482:I:ANY] ieee80211_oce_vdetach: OCE terminated
[ 3399.366498]
[ 3399.452818] wlan: [5524:I:MBSSIE] osif_mbssid_sanity_check: mbssid_sanity_ok: YES
[ 3399.452865] wlan: [5524:I:ANY] osifp_create_wlan_vap: VDEV Create 00:06:ae:6d:b5:3b
[ 3399.460047] wlan: [5524:I:ANY] wlan_vap_create: devhandle=0x90ba0500, opmode=IEEE80211_M_HOSTAP, flags=0x1
[ 3399.460047]
```

Figure 50: Kernel Log Tab

S.No.	Field	Description
1.	Kernel Logs	Kernel Logs are displayed to the end-users.

Table 41: Kernel Log Description

5.9.4 Tools

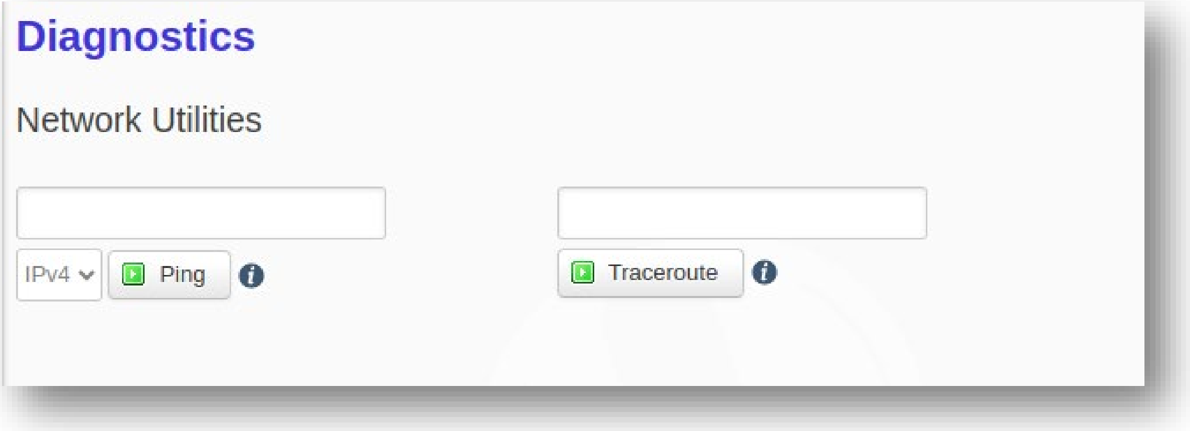


Figure 51: Tools

S.No.	Field	Description
1.	Tools	Enables end users to debug and troubleshoot as per arising needs.

Table 42: Tools Description

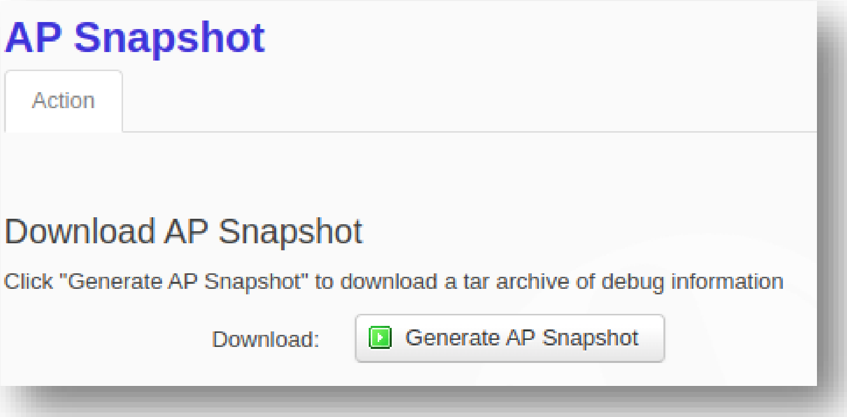
5.9.5 Associated Stations

The list of connected clients along with the relevant information in respective information columns is populated in this screen. A basic overview of the screen to show connected clients is given below:

S.No.	Field	Description
1.	Associated Stations	Through this, end users can see the listings of the Client device details which are connected to the network.

Table 43: Associated Stations Description

5.9.6 AP Snapshots



AP Snapshot

Download AP Snapshot

Click "Generate AP Snapshot" to download a tar archive of debug information

Download: Generate AP Snapshot

Figure 52: Download AP Snapshots

S.No.	Field	Description
1.	AP Snapshots	AP snapshots can be downloaded after generation.
2.	Download AP Snapshot	The AP snapshot after generation will be downloaded by the user
3.	Generate AP Snapshot	AP Snapshot is generated.

Table 44: AP Snapshot Description

5.10Switch AP Mode

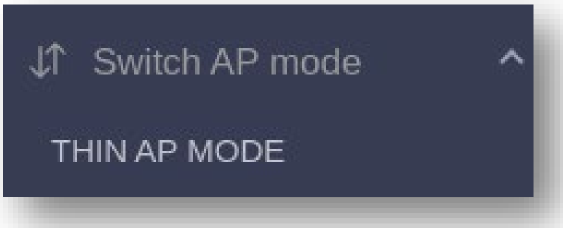


Figure 53: Switch AP Mode

S.No.	Field	Description
1.	Switch AP Mode	End users have the option to enable thick or thin mode graphic user interface.

Table 45: Switch AP Mode Description

5.11 Logout

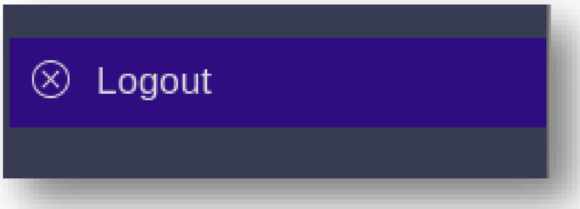


Figure 54: Logout

S.No.	Field	Description
1.	Logout	Users can log out of the GUI after editing configuration according to their specific requirements.

Table 46: Logout Description

Note: The user can download the **UcNMS** User Guide from io.hfcl.com for detailed configuration and management, when the APs are operating in Thin/Managed mode.

Copyright Notice

Legal Disclaimer

The information contained in this document is subject to change without notice. The information in this document is provided for informational purposes only. HFCL Limited specifically disclaims all warranties, express or limited, including, but not limited, to the implied warranties of merchantability and fitness for a particular purpose, except as provided for in a separate software license agreement.

About HFCL Limited

HFCL is a leading technology company specializing in creating digital networks for telcos, enterprises, and governments. Over the years, HFCL has emerged as a trusted partner offering sustainable high-tech solutions with a commitment to provide the latest technology products to its customers. Our strong R&D expertise coupled with our global system integration services and decades of experience in fibre optics enable us to deliver innovative digital network solutions required for the most advanced networks.

The Company's in-house R&D Centers located at Gurgaon & Bengaluru along with invested R&D Houses and other R&D collaborators at different locations in India and abroad, innovate a futuristic range of technology products and solutions. HFCL has developed capabilities to provide premium quality Optical Fiber and Optical Fiber Cables, state-of-the-art telecom products including 5G Radio Access Network (RAN) products, 5G Transport Products, WiFi Systems (WiFi 6, WiFi 7), Unlicensed Band Radios, Switches, Routers and Software Defined Radios.

The Company has state-of-the-art Optical Fiber and Optical Fiber Cable manufacturing plants at Hyderabad, Optical Fiber Cable manufacturing plant in Goa and in its subsidiary HTL Limited at Chennai.

We are a partner of choice for our customers across India, Europe, Asia Pacific, Middle East, Africa, and USA. Our commitment to quality and environmental sustainability inspires us to innovate solutions for the ever-evolving customer needs.

Correspondence

HFCL Limited
8, Commercial Complex,
Masjid Moth, Greater Kailash II,
New Delhi-110048,
India Tel: +91-11-30882624/2626

Mail us at:

Sales: iosales@hfcl.com

Enquiry: ioenquiry@hfcl.com

Support: iosupport@hfcl.com

Toll Free (Domestic): 8792701100

Revision History

Date	Rev No.	Description	Reviewed By	Approved By
01/09/2023	A0-00	Initial Draft Release	Shashank Sejwal	Prasad Balakrishnan